PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MÁSTER EN REDES DE COMUNICACIÓN

TEMA:

“DISEÑO DE UN SISTEMA DE GESTIÓN, CONTROL Y MONITOREO PARA LA RED DE INFOCENTROS A NIVEL NACIONAL”

ENTIDAD BENEFICIARIA:

MINISTERIO DE TELECOMUNICACIONES DE LA SOCIEDAD DE LA INFORMACIÓN

DANILO MAURICIO ROSERO PADILLA

Quito, agosto de 2015

Contenido

CAPÍTULO I
SUSTENTO TEÓRICO

1.1 [1]INTRODUCCIÓN

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), busca automatizar procesos administrativos, técnicos y operativos propios de su gestión, de forma tal que contribuyan al desarrollo humano, social, laboral y al mejoramiento de la prestación de servicios tecnológicos, en base a una adecuada infraestructura tecnológica, red de servicios y sistemas integrados de información, que permitan: eficiencia, productividad, calidad y oportunidad en los servicios ofrecidos, como medios que apoyan al cumplimiento de la Misión, la Visión y los Valores Corporativos de la Organización.

La modernización incluye la disponibilidad de los servicios a través del Internet mediante algunas aplicaciones. La instalación de computadores a nivel nacional hace que se generen una gran cantidad de requerimientos de soporte tecnológico los cuales deben ser gestionados de acuerdo a la aplicación de prácticas internacionales de servicio y soporte al usuario, con el apoyo de herramientas informáticas de software que permitan el registro, y el seguimiento de dichos requerimientos, así como el control y gestión de los servicios tecnológicos.

La herramienta de software que necesita el Ministerio de Telecomunicaciones de la Sociedad de la Información (MINTEL), debe permitir automatizar los procesos de servicio, control, gestión y soporte tecnológicos con el objetivo de dar trámite a la gran cantidad de requerimientos provenientes de los diferentes infocentros a nivel nacional, con el propósito de enmarcarse en un plan de aprovechamiento de los recursos tecnológicos existentes y a través de ellos poder optimizar los recursos instalados, determinar las necesidades actuales

y futuras, para planificar, medir y optimizar las capacidades requeridas por parte de los beneficiarios directos, y en general formalizar la administración tecnológica, para ello es necesario efectuar un análisis adecuado para la Implantación de Buenas Prácticas de Administración Tecnológica en Áreas de Producción basados en ITIL.

Uno de los puntos importantes en este proyecto es el aseguramiento de la calidad a nivel nacional mediante el manejo de incidencias y proveer las soluciones en el tiempo y lugar adecuados conforme a los SLA's definidos, para lo cual es necesario previamente un análisis de la situación actual que nos permita conocer las debilidades, con el objetivo de alcanzar la eficiencia en la Gestión de TI y determinar los procesos necesarios para administrar el área de TI con el fin de garantizar la integración de los servicios.

1.2 JUSTIFICACIÓN

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), como ente rector de las telecomunicaciones, en cumplimiento de la Estrategia Ecuador Digital 2.0 y su Plan de Acceso Universal, instaló 775 e implementará 703 infocentros a nivel nacional.

Los infocentros instalados se encuentran en zonas rurales y urbano marginales a nivel nacional, permitiendo el acceso a tecnologías de la información y comunicaciones a persona de escasos recursos económicos, de igual manera se brinda capacitaciones continuas en alistamiento digital contribuyendo con la disminución de la brecha digital dentro de estas zonas.

Dentro de los problemas que actualmente se generan en los infocentros al no existir procesos estructurados y un software adecuado que permita integrar la gestión administración, control y monitoreo de toda la infraestructura entregada y servicios de

conectividad, causando incertidumbre sobre el verdadero uso de los infocentros por lo que ha crea desconfianza entre las autoridades para la ejecución de nuevos proyectos.

Se ha determinado que varios de los beneficiarios de los infocentros y proveedores de servicios contratados no cumplen con los parámetros establecidos para una administración adecuada de los equipos y servicios entregados por el MINTEL, por lo que se obtiene como resultado los siguientes inconvenientes:

1. Un servicio Caótico.
    - No existen procesos estándar
    - No hay Operaciones de TI
    - No hay llamadas de notificación por parte de los usuarios
    - No existe control real de la existencia ni uso de los equipos provistos.
2. Inconsistencias en la Información
    - Topologías diferentes
    - Inventarios diferentes
    - No existe una consolidación de Gestión
    - No hay métodos para asegurar la conformidad con los procesos, como;
        i. Rendimiento
        ii. Cambios
        iii. Problemas
        iv. Configuración
        v. Disponibilidad
        vi. Automatización

Con el fin de estimular el uso y mejora de procesos exitosos de gestión de tecnología es necesario desarrollar e implementar un Sistema de Monitoreo evaluativo por resultados; que fortalezca la gestión de los proyectos implementados por el MINTEL.

En vista de los inconvenientes que se han generado por la falta de control se ha visto la necesidad de implementar el proyecto a través de la creación de un centro de monitoreo, administración y gestión de todos los servicios e infraestructura tecnológica basados en las prácticas mundiales ITIL, de igual manera con los proveedores de los servicios contratados; con el fin de contar con una herramienta para la toma de decisiones y garantizar el uso eficiente de los recursos entregados por el MINTEL, ya que nos proporcionará información actualizada y detallada del uso de los bienes y servicios tecnológicos entregados.

Adicionalmente se podrán determinar políticas y procesos mediante un conjunto de estándares que permitan administrar cada uno de los infocentros instalados convirtiéndose en una estrategia fundamental del MINTEL en el uso adecuado de la administración de los recursos. Mentalizar el concepto de servicio a los beneficiarios, tener servicios sólidos y estandarizados, saber los costos del servicio, y tener criterios de mejora medibles estableciendo índices de rendimiento.

Mantener una herramienta automática donde se registren los incidentes y problemas ocurridos durante el día, incluyendo la manera como se dio solución y el nombre del usuario que solicitó la ayuda, a esta herramienta debe acceder todo el personal de Mesa de Ayuda, para si en caso se presente el mismo problema dar solución rápidamente.

Tener una consola de requerimientos integrada al "*Service Desk*" local para dar servicios integrales de Gestión, atender solicitudes y poder proveer un catálogo de servicios a los beneficiarios.

Mantener herramientas de gestión y monitoreo que permitan tener un control de las aplicaciones críticas de manera activa que ayude a prevenir e identificar las fallas

tecnológicas a tiempo, de tal manera que permita a la Dirección de Acceso Universal ofrecer alta disponibilidad de sus servicios y tener continuidad en los proyectos.

Tener una consola de gestión que permita tener el control de cada dispositivo entregado a cada punto beneficiario mediante la Gestión de control Remoto, Distribución de *"Software"* y control de accesos e inventarios.

1.3 ANTECEDENTES.[2]

Mediante Decreto Ejecutivo No. 8, del 13 de agostos del 2009, publicado en el Registro Oficial No. 10 de 24 de agosto de 2009, el señor Presidente Constitucional de la República creó el Ministerio de Telecomunicaciones y de la Sociedad de la Información reestructurando el esquema institucional del sector de la telecomunicaciones en el Ecuador, otorgando al Ministerio de Telecomunicaciones y de la Sociedad de la Información la rectoría del sector.

La Constitución de la República del Ecuador, dentro de los derechos del Buen Vivir reconoce a todas las personas, en forma individual o colectiva, el derecho al acceso universal a las tecnologías de la información y comunicaciones; y pone énfasis en aquellas personas y colectividades que carecen o tengan acceso limitado a dichas tecnologías y obliga al Estado a "incorporar las tecnologías de la información y comunicaciones en el proceso educativo y propiciar el vínculo de la enseñanza con las actividades productivas o sociales". De allí, que en la perspectiva de profundizar el nuevo régimen de desarrollo, se hace necesario ampliar la visión sobre la conectividad y las telecomunicaciones considerando como un medio para contribuir a alcanzar los objetivos del Régimen de Desarrollo y se enmarca dentro de los

[2] Fuente: Registro Oficial, https://www.registroficial.gob.ec/

objetivos y metas del Plan Nacional para el Buen Vivir 2009-2013 específicamente en el Objetivo 2: “Mejorar las capacidades y potencialidades de la ciudadanía”.

En consecuencia, la acción estatal en los próximos años deberá concentrarse en tres aspectos fundamentales: Conectividad, dotación de hardware y el uso de la TIC para la Revolución Educativa.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información mediante su estrategia Ecuador Digital 2.0 y su Plan de Acceso Universal ha desarrollado y ejecutado proyectos de implementación de laboratorios de cómputo en establecimientos educativos fiscales y de infocentros comunitarios ubicados en las zonas rurales a nivel Nacional con el fin de permitir el acceso a los estudiantes y a la ciudadanía en general de dichas zonas, a las Tecnologías de la Información y Comunicación, y dar cumplimiento a los objetivos planteados en el Plan Nacional de Desarrollo que busca mejorar la calidad de la educación en el Ecuador y un incremento en la matriz productiva, reducir la brecha digital y brindar a la población de las zonas rurales la igualdad de oportunidades de desarrollo.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

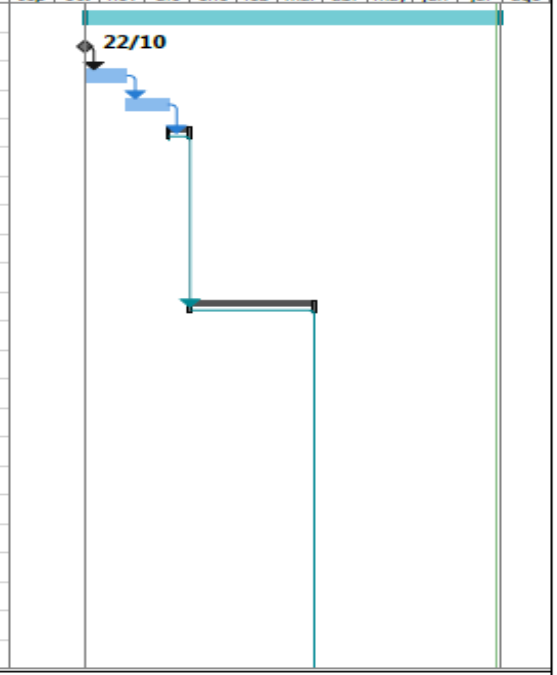
- Diseñar un sistema integrado para la gestión, control y monitoreo de la infraestructura tecnológica así como de los servicios entregados a nivel nacional a los beneficiarios del programa infocentros, que permitan identificar los eventos, impacto y desempeño, para asegurar la calidad del servicio entregado, durante la vida útil de los proyectos.

1.4.2 OBJETIVOS ESPECÍFICOS

- Establecer los modelos de gestión que permiten el correcto funcionamiento de la red infocentros a nivel nacional.
- Contar con herramientas de control y monitoreo que permitan garantizar una administración eficiente red infocentros.
- Garantizar el buen desempeño de la red a través de tareas, reglas y políticas que permiten cumplir los procesos preestablecidos.
- Dimensionar las instalaciones físicas y estaciones de trabajo con el más avanzado software para brindar una mejor administración y desempeño de las herramientas.
- Definir el personal necesario para llevar a cabo tareas como de administración, supervisión, monitoreo y mantener en óptimas condiciones la red de infocentros a nivel nacional.

1.5 CRONOGRAMA.

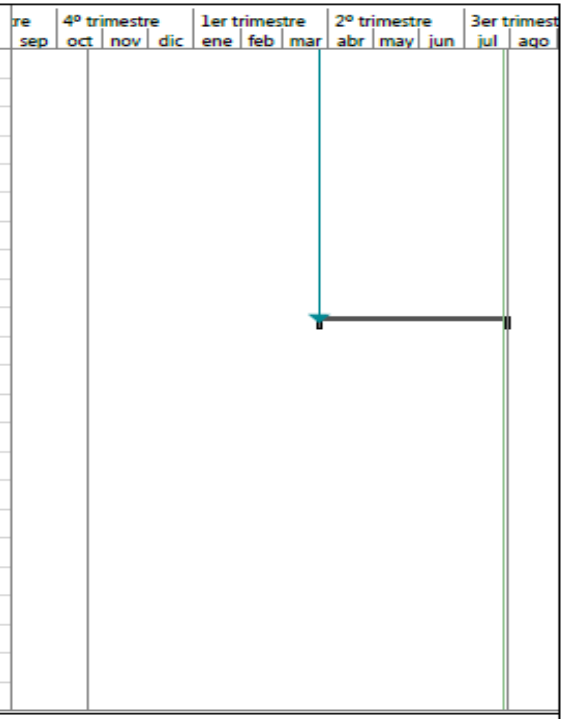
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		**CRONOGRAMA PARA EL DISEÑO DE UNA SISTEMA DE CONTROL, MONITOREO Y DISTRIBUCIÓN DE CONTENIDOS PARA LA RED INFOCENTROS**	**201 días?**	**mié 22/10/14**
2		APROBACIÓN DEL TEMA	0 días	mié 22/10/14
3		ELABORACIÓN DEL PLAN DE TESIS	20 días	mié 22/10/14
4		RECOPILACIÓN DE LA INFORMACIÓN REQUERIDA	20 días	mié 19/11/14
5		**FASE DE PLANIFICACIÓN**	**11 días**	**mar 16/12/14**
6		ANÁLISIS DE REQUERIMIENTOS DEL SISTEMA		
7		ANÁLISIS COMPARATIVO DE SOLUCIONES EXISTENTES		
8		COMPARATIVA DE ALTERNATIVAS DE IMPLEMENTACIÓN		
9		ALTERNATIVA NACIONAL		
10		PRODUCTOS OFERTADOS		
11		**FASE DE EJECUCIÓN**	**60 días**	**mié 31/12/14**
12		DISEÑO DE LA ARQUITECTURA		
13		COMPONENTES DE MONITOREO DE RED Y EQUIPAMIENTO INFORMÁTICO		
14		COMPONENTES PARA EL CONTROL DE ACCESO Y NAVEGACIÓN		
15		COMPONENTES PARA DISTRIBUCIÓN DE CONTENIDOS		
16		ALTERNATIVAS DE IMPLEMENTACIÓN DE COMPONENTES		
17		SERVICIOS EN LA NUBE		
18		IMPLEMENTACIÓN DE INFRAESTRUCTURA PROPIA		
19		IMPLEMENTACIÓN HÍBRIDA		
20		SOLUCIÓN APLICADA A NUESTRO DISEÑO		
21		MÓDULOS		
22		ARQUITECTURA Y ADMINISTRACIÓN		
23		SEGURIDAD Y ACCESO		



Proyecto: Proyecto1
Fecha: lun 27/07/15

Tarea	Resumen inactivo	Tareas externas
División	Tarea manual	Hito externo
Hito	solo duración	Fecha límite
Resumen	Informe de resumen manual	Progreso
Resumen del proyecto	Resumen manual	Progreso manual
Tarea inactiva	solo el comienzo	
Hito inactivo	solo fin	

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
24		ACUERDOS DE NIVELES DE SERVICIO		
25		MAPA DE SERVICIO		
26		MESA DE AYUDA (SERVICE DESK)		
27		GESTIÓN DE INCIDENTES		
28		GESTIÓN DE NIVELES DE SERVICIO		
29		REPORTES		
30		GESTIÓN DE ACTIVOS		
31		MEDICIÓN DE TRÁFICO		
32		CONTROL REMOTO		
33		**FASE DE ELABORACIÓN DOCUMENTAL**	**90 días**	**mié 25/03/15**
34		ELABORACIÓN DEL DOCUMENTO FINAL		
35		**FASE DE CIERRE**		
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				



Proyecto: Proyecto1
Fecha: lun 27/07/15

Tarea	Resumen inactivo	Tareas externas
División	Tarea manual	Hito externo
Hito	solo duración	Fecha límite
Resumen	Informe de resumen manual	Progreso
Resumen del proyecto	Resumen manual	Progreso manual
Tarea inactiva	solo el comienzo	
Hito inactivo	solo fin	

Página 2

CAPÍTULO II

ESTADO DEL ARTE

2.1 ANTECEDENTES.

A través de este diseño se busca proporcionar al Ministerio de Telecomunicaciones y de la Sociedad de la Información, una herramienta que permita automatizar procesos administrativos, técnicos y operativos propios de su gestión, de forma tal que contribuyan al desarrollo humano, social, laboral y el mejoramiento de la prestación de servicios tecnológicos, a través de una adecuada infraestructura tecnológica, red de servicios y sistemas integrados de información, que permitan: eficiencia, productividad, calidad y oportunidad en los servicios ofrecidos, como medios que apoyan al cumplimiento de la Misión, la Visión y los Valores Corporativos .

Dentro de los procesos de modernización incluyen la disponibilidad de los servicios a través del Internet mediante la utilización de algunas aplicaciones para la actualización de los conocimientos. La instalación de miles de computadores, *"thin client"* y servidores a nivel nacional generan una gran cantidad de requerimientos de soporte tecnológico los cuales deben ser gestionados de acuerdo a las mejores prácticas internacionales de servicio y soporte al usuario, con el apoyo de herramientas informáticas de software que permitan el registro, el seguimiento de dichos requerimientos, el control y gestión de los servicios tecnológicos.

La herramienta de software que requiere el MINTEL debe permitir automatizar los procesos de servicio, control, gestión y soporte tecnológicos para dar trámite de manera eficiente a la gran cantidad de requerimientos provenientes de las diferentes infocentros a nivel

nacional y con el propósito de enmarcarse en un plan de aprovechamiento de los recursos tecnológicos existentes y a través de ellos poder optimizar los recursos instalados, determinar las necesidades actuales y futuras, planificar medir y optimizar las capacidades requeridas por parte de los beneficiarios directos, y en general formalizar la administración tecnológica, para ello es necesario efectuar un análisis adecuado para la Implantación de Buenas Prácticas de Administración Tecnológica en Áreas de Producción basados en ITIL.

Uno de los puntos importantes en este proyecto es el aseguramiento de la calidad a nivel nacional mediante el manejo de incidencias y proveer las soluciones en el tiempo y lugar adecuados conforme a los SLA's definidos, para lo cual es necesario previamente un análisis de la situación actual que nos permita conocer las debilidades actuales para hacer más eficiente la Gestión de IT, describir los procesos necesarios para administrar el área de TI eficazmente con el fin de garantizar la integración de los servicios.

2.2 ANÁLISIS DEL ESTADO ACTUAL DE LA RED.[3]

2.2.1 INFOCENTROS:

Se define como un espacio social donde se garantiza el acceso de los individuos a las Tecnologías de la Información y Comunicación, a través de equipamiento informático e internet; apalancando la participación, organización y el protagonismo de los sectores populares, en el contexto de un desarrollo social integrado y estructurado.

2.2.2 OFERTA DE INFOCENTROS

Constituye en la cantidad de infocentros implementados hasta el 2015, adicionalmente se contemple la implementación de 703 infocentros en el periodo 2017, la tabla 1 detalla el número de infocentros implementados hasta el 2014 por proyecto y provincia.

[3]Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL.

Tabla 1 Número de Infocentros por Provincia y Proyecto[4]

PROVINCIAS	INFOCENTROS PAUTIC	INFOCENTROS ECUADOR ESTRATÉGICO	INFOCENTROS AMPLIACIÓN RED INFOCENTROS	MEGAINFOCENTROS AMPLIACIÓN RED INFOCENTROS	INFOCENTROS DONACIONES
Azuay	41	3	3	1	0
Bolívar	13	0	5	0	1
Cañar	3	0	4	1	0
Carchi	10	0	20	2	0
Chimborazo	40	0	26	3	0
Cotopaxi	23	0	16	1	0
El Oro	22	6	16	0	0
Esmeraldas	6	10	17	1	1
Galápagos	0	0	0	0	0
Guayas	2	0	32	1	9
Imbabura	36	0	4	1	1
Loja	30	0	17	0	2
Los Ríos	9	0	5	2	0
Manabí	21	14	26	3	1
Morona Santiago	14	17	1	1	0
Napo	18	8	1	0	0
Orellana	11	9	0	0	0
Pastaza	11	8	3	0	0
Pichincha	22	0	23	3	2
Santa Elena	6	0	11	0	0
Santo Domingo de los Tsáchilas	8	0	16	1	0
Sucumbíos	14	10	2	0	0
Tungurahua	12	0	19	3	0
Zamora Chinchipe	1	15	0	0	0
Zonas no delimitadas	0	0	0	0	0
TOTAL GENERAL	**373**	**100**	**267**	**24**	**17**

2.2.3 UBICACIÓN E IMPACTO TERRITORIAL.

2.2.3.1 COBERTURA DEL PROYECTO.

La cobertura del proyecto abarca a zonas rurales y urbanos marginales a nivel nacional ya que incorpora cada año a nuevos beneficiarios en base a las necesidades de cada provincia.

En el Anexo 001 se encuentra el listado de las instituciones beneficiarías del 2010 hasta el 2014. Estos listados incluyen entre otros datos: Provincia, Cantón Parroquia, Dirección.

[4]Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, Dirección de Accesos universal.

2.2.4 REGISTRO DE LA TOPOLOGÍA.

Se define como topología de red a la disposición física en la que se conecta una red de dispositivos tecnológicos, en la red de infocentros a nivel nacional, se cuenta con dos tipos de topologías de red:

Red en Estrella, es la cual las estaciones están conectadas directamente al *"switch"*, todas las comunicaciones se realizan necesariamente a través de él. Todas las estaciones están conectadas por separado a un *"switch"*, pero no están conectadas entre sí. Esta red crea una mayor facilidad de gestión, control y monitoreo de la información, el cual gestiona la redistribución de la información. La desventaja de este tipo de redes es el costo del cableado, ya que puede llegar a ser alto. Su punto débil consta en el*"switch"* ya que es el que sostiene la red. Se dispone de este tipo de topología en 291 infocentros que corresponden al proyecto Ampliación de la Red Infocentros.

Red Inalámbrica WI-FI, cumple con los estándares IEEE 802.11x, las redes inalámbricas hacen posible que se puedan conectar las estaciones sin la necesidad de instalaciones cableadas. Se dispone de este tipo de topología en 490 infocentros que corresponden a los proyectos PAUTIC, Ecuador Estratégico y Donaciones.

2.2.5 TIPO DE TECNOLOGÍA INSTALADA.

La tecnología instalada difiere en base al proyecto en el que fue implementado, es así que el proyecto PAUTIC, Ecuador Estratégico y Donaciones manejan una arquitectura en base a Computadoras Personales a diferencia del proyecto Ampliación de la Red Infocentros el cual maneja una arquitectura cliente servidor, es importante realizar este análisis independiente ya que el sistema de control, gestión y monitoreo que estaremos diseñando deberá ser compatible con los dos tipo de arquitectura implementada.

2.2.5.1 PAUTIC, ECUADOR ESTRATÉGICO Y DONACIONES

Estos proyectos plantean que las entidades beneficiarias puedan contar con las herramientas tecnológicas modernas, para desplegar el plan nacional de alistamiento digital, en la Tabla 2 Equipamiento Entregado, se refleja el equipamiento entregado en estos proyectos, en la Tabla 3. Tipo y Cantidad de Equipamiento, se definen la cantidad de equipamiento.

Tabla 2Equipamiento Entregado Periodo 2010 al 2012 [5]

EQUIPAMIENTO ENTREGADO DEL AÑO 2010 AL 2012
Computadoras
Proyectores
Soporte Techo Proyector
Router/Switch
Pizarra
Impresoras
Alarma
Sillas/Escritorio
Reguladores/UPS
Tóner/Suministro
Cables VGA
Cables VGA - EN Y
Aire Acondicionado

Tabla 3Tipo y Cantidad de Equipamiento[6]

					EQUIPAMIENTO INFOCENTROS										
CANTIDAD Y TIPO DE EQUIPAMIENTO		NÚMERO TOTAL DE SITIOS	DESCRIPCIÓN DEL SITIO	# PC POR TIPO	COMPUTADORAS	PROYECTORES (1)	IMPRESORAS (1)	VIDEOGRABADORA (1)	WIRELESS ACCESS POINT (1)	REGULADORES (1)	TONNER / SUMINISTROS (1)	CABLES VGA (1)	SOPORTE DE PARED (1)	BANDEJA PARA SOPORTE (2)	CABINAS TELEFÓNICAS EQUIPAMIENTO (2)
INFOCENTROS	TIPO 1	200	INFOCENTROS A IMPLEMENTAR	6	1200	200	200	200	200	1200	200	200	200	400	400
	TIPO 2	163	INFOCENTROS A IMPLEMENTAR	9	1467	163	163	163	163	1467	163	163	163	326	326
	TIPO 3	10	INFOCENTROS A IMPLEMENTAR	18	180	10	10	10	10	180	10	10	10	20	20
TOTAL INFOCENTRO		**373**			**2847**	**373**	**373**	**373**	**373**	**2847**	**373**	**373**	**373**	**746**	**746**
Equipamiento Adicional que se Instalará en Escuelas**					**1073**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTAL EQUIPAMIENTO					**3920**	**373**	**373**	**373**	**373**	**2847**	**373**	**373**	**373**	**746**	**746**

2.2.5.2 AMPLIACIÓN DE LA RED INFOCENTROS

Este proyecto plantea que las entidades beneficiarias puedan contar con las herramientas tecnológicas modernas, de menor costo y mayor tiempo de vida útil que el equipamiento

[5]Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, Dirección de Accesos universal.

[6]Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, Dirección de Accesos universal y Dirección de Acceso Universal

entregado en los proyectos anteriores, por tal sentido el MINTEL optó por una solución cliente servidor, en la Tabla 3. Equipamiento Entregado ARI, se define el equipamiento entregado en a través del proyecto.

Tabla 4Equipamiento Entregado Periodo 2014 al 2015[7]

ÍTEM	CANTIDAD	COMPONENTE
EQUIPAMIENTO		
1	1	SERVIDOR INFOCENTRO
2	10	THIN-CLIENT
3	1	PROYECTOR
4	1	IMPRESORA MULTIFUNCIÓN SISTEMA DE TINTA CONTINUA
5	1	SWITCH DE RACK INFOCENTRO
6	1	REGULADOR PRINCIPAL
7	10	REGULADORES DE VOLTAJE PARA THIN CLIENT
8	1	SISTEMA DE ALARMA
9	1	VIDEO CÁMARA DIGITAL
10	1	AIRE ACONDICIONADO
11	1	TELEVISOR 42"
12		CABLEADO ESTRUCTURADO Y ACCESORIOS
13		CABLEADO ELÉCTRICO Y ACCESORIOS
SOFTWARE		
14	1	Windows Server 2012R2 para proyectos educativos
15	10	Windows Server CAL 2012 para proyectos educativos
16	1	LINUX (Servidor y Thin Client) última versión estable
17	10	Office 2013 Professional (3 años) para proyectos educativos
MOBILIARIO		
18	1	MUEBLE PARA EL PUESTO DEL FACILITADOR
19	10	MUEBLE PARA COMPUTADOR-ESTACIONES DE TRABAJO
20	1	MUEBLE PARA IMPRESORA
21	10	MESAS PARA SALA DE CAPACITACIÓN
22	31	SILLAS METÁLICAS SIN BRAZOS
23	1	PIZARRA DE TIZA LÍQUIDA ANTIREFLEJANTE
24	1	SEÑALÉTICA
SERVICIOS		
25	1	CAPACITACIÓN (EN GRUPOS DE 10 BENEFICIARIOS)
26	1	INSTALACIÓN EN SITIO
27	1	GARANTÍAS TÉCNICAS (3 Años)
28	1	MANTENIMIENTO PREVENTIVO/CORRECTIVO Y SOPORTE TÉCNICO (3 años)
29	1	CONECTIVIDAD INTERNET (CNT EP)
30	1	SERVICIO DTH PAQUETE BÁSICO (CNT EP)

2.2.6 LUGARES DE INSTALACIÓN.

- 1 sitio central de control.(PICHINCHA-QUITO- MINTEL)
- 781 sitios donde se contempla la implementación el sistema de gestión, control y monitoreo a nivel nacional (listado de Infocentros se adjunta en el Anexo 001).

[7]Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, Gerencia de Proyecto Emblemático Ampliación de la Red Infocentros.

- 703 lugares sin definir al momento donde se contempla la implantación de infocentros a nivel nacional

2.2.7 TIPO DE CONECTIVIDAD.

Dado que la conectividad de todos los proyectos a través de los cuales se implementa infocentros está dada por la Corporación Nacional de Telecomunicaciones CNT EP, todos manejan el mismo tipo de conectividad (ADSL, VSAT y Fibra Óptica).

Tabla 5Planes y Tarifas de Conectividad disponibles en la CNT EP para clientes sociales. [8]

PLAN	DENOMINACIÓN	INSCRIPCIÓN O INSTALACIÓN	MENSUAL
A-INTERNET PLAN PARA INFOCENTROS	ADSL Corporativo 2048x768 Kbps con COBRE	$ 80.00	$ 50.00
B-INTERNET PLAN PARA INFOCENTROS	ADSL Corporativo 3000x768 Kbps con COBRE	$ 80.00	$ 55.00
C-INTERNET PLAN PARA INFOCENTROS	ADSL Corporativo 3000x768 Kbps con FIBRA	$ 120.00	$ 55.00
D-INTERNET PLAN PARA MEGAINFOCENTROS	Pymes Asimétrico 10 x 5Mbps con FIBRA	$ 120.00	$ 140.00
E-DTH (Televisión Satelital) PLAN BÁSICO CON 55 CANALES DE TV TARIFA CORPORATIVA	Plan Gold Corporativo SD	$ 20.00	$ 10.00
F-VSAT REINSTALACIÓN DE PAUTIC TARIFA MENSUAL CON CARGO A PAUTIC	Banda Ku 1024/512 Kbps 4:1	$ 1,116.60	$ 1,116.60
MIGRACIÓN VSAT INCLUYE IVA	acceso terrestre	$ 954.24	80%
ADICIONALES	acceso terrestre más aéreo	$ 1,636.32	10%
	acceso terrestre más bote	$ 1,895.79	10%
	Galápagos 1 (Sta. Cruz/San Cristóbal)	$ 1,209.60	
	Galápagos 2 (otras islas)	$ 2,004.80	
	PROMEDIO PONDERADO (SIN GALÁPAGOS)	$ 1,116.60	

Se dispone de una solución cuya plataforma de transmisión de datos es TCP/IP utilizando sistemas de última generación que permitan la operatividad de los infocentros y para que

[8] Fuente: Datos obtenidos de la Jefatura de Inclusión Social CNT EP.

puedan soportar diferentes tipos de aplicaciones y tráfico de información como acceso a Internet, transmisión de datos, video conferencia y voz, permitiendo la priorización de tráfico y aplicación de políticas de Calidad de Servicio a nivel de las capas superiores del modelo TCP/IP (red y aplicación).

A continuación se dan las especificaciones generales que tiene los canales de comunicaciones, las mismas son aplicadas tanto para el componente VSAT, componente F.O como para el componente proyecto ADSL:

2.2.7.1 CONECTIVIDAD A CLIENTES SOCIALES MEDIANTE TECNOLOGÍAS ADSL

La infraestructura de acceso más importante que posee CNT EP para acceso a Internet está constituida principalmente por su plataforma ADSL la cual permite llegar a los usuarios con capacidades importantes de conexión utilizando el par de cobre como medio de transporte.

CNT EP, es una empresa que provee productos y servicios de telecomunicaciones convergentes, posibilitando así el acceso a los ciudadanos a la banda ancha y tecnologías de la información y de las comunicaciones, impulsando su uso a nivel nacional.

Dentro de la Tecnología que dispone CNT EP, se puede destacar:

Backbone

Teniendo unos anillos de Fibra óptica mono modo que cubre alrededor de 10.000 km del territorio nacional, la cual opera conforme a estándares internacionales, tales como 568B.3.1.

Red de Transporte

Está montada con IP/MPLS y DWDM, la cual esta implementada casi en su totalidad con tecnología CISCO, disponiendo de interfaces de conexión con capacidad de hasta 10Mmps.

Conectividad Internacional

Pose el nivel de TIER 2, con lo cual dispones de una conectividad internacional de capacidad de transporte de datos de 192 STM-1

2.2.7.2 CONECTIVIDAD A CLIENTES SOCIALES MEDIANTE TECNOLOGÍAS VSAT

Considerando que la infraestructura para la provisión del servicio de internet que poseen los operadores de telecomunicaciones CNT EP., no permite llegar a los clientes sociales objetivo de los infocentros, mediante tecnologías de acceso alámbricas (ADSL), inalámbricas (WiMax)o distintos tipos de enlaces terrestres, fue necesario plantear una solución tecnológica que permita solventar esta limitación y por tanto que permita cumplir con los objetivos planteados en los distintos Proyectos para la implementación de Infocentros Comunitarios. Esta solución tecnológica corresponde al mejoramiento y el desarrollo de la infraestructura satelital para acceso mediante estaciones VSAT en Banda Ku.

La solución contempla la implementación de la infraestructura satelital que en complemento con la existente de la CNT EP permita coadyuvar al cumplimiento de los objetivos de los infocentros.

Tabla 6Planes y Tarifas de Conectividad VSAT.[9]

Tarifas del Producto	Compartición	Tarifa Mensual TECHO	Tarifa Mensual MEDIO	Tarifa Mensual PISO
256 / 128 Kbps	2:1	$ 613	$ 531	$ 468
512 / 256 Kbps	2:1	$ 894	$ 775	$ 684
1024 / 512 Kbps	2:1	$ 1.458	$ 1.264	$ 1.115
2048 / 1024 Kbps	2:1	$ 2.585	$ 2.240	$ 1.977
256 / 128 Kbps	4:1	$ 356	$ 342	$ 329
512 / 256 Kbps	4:1	$ 614	$ 532	$ 469
1024 / 512 Kbps	4:1	$ 894	$ 775	$ 684
2048 / 1024 Kbps	4:1	$ 1.458	$ 1.264	$ 1.115

Table7 Características técnicas de Conectividad Satelital Vsat Banda Ku.

CARACTERÍSTICA DEL PRODUCTO	OFERTA VIGENTE	NUEVA OFERTA
Compartición	No existe oferta en banda Ku. Se ofertan planes VSAT en Banda C (1:1, 2:1, 4:1, 8:1) y también se ofertan planes en SCPC	2:1 4:1
Velocidad de Bajada	Hasta 1024 Kbps en VSAT Banda C Hasta 768 Kbps en SCPC	Hasta 2048 Kbps
Planes	Planes VSAT Banda C: 128 x 128 Kbps 256 x 256 Kbps 512 x 512 Kbps 1024 x 512 Kbps Planes SCPC simétricos: 64, 128, 192, 256, 384, 512, 768 Kbps	256 x 128 Kbps 512 x 256 Kbps 1024 x 512 Kbps 2048 x 1024 Kbps

2.3 MODELOS DE GESTIÓN.

Se concibe como el conjunto de tareas o acciones encaminadas a alcanzar objetivos, a través del cumplimiento y la óptima aplicación de procesos.

2.3.1 GESTIÓN DE RED

La gestión de red se inicia en los años 1980 en donde no se contaba con un soporte real y bien definido, las herramientas de gestión de red con la que se contaba eran ICMP, PING y Treceroute. En la actualidad se cuenta con el estándar SNMP, dado el crecimiento global de las redes se requiere la utilización de una serie de ampliaciones a este estándar como los

[9] Fuente: Datos obtenidos de la Jefatura de Inclusión Social CNT EP.

son: RMON (Remote Monitor) el cual es un monitor a nivel de subredes y no solo a nivel de nodos y el desarrollo de SNMP versión 2 y 3.

2.3.1.1 MODELOS DE GESTIÓN DE RED

Para definir el modelo de gestión de red debemos comenzar por lo elementos de gestión:

a) Estación de gestión, es la interface entre el usuario y el sistema de gestión, deberá poseer un acceso en modo gráfico, acceso a las MIB's (*"Management Information Base"*) y capacidad de creación de órdenes de monitorización concretas, recolección de información y toma de informaciones.

b) Agente, es una abstracción de software que actúa y permite la gestión de un dispositivo.

c) Base de Información de Gestión MIB's, base de datos la cual contiene información en niveles jerárquicas, estructurados en forma de árbol, en estas podemos encontrar información de todos los dispositivos gestionados en una red de comunicaciones.

d) Protocolo de Gestión de Red (SNMP), son aquellos que definen la comunicación entre los nodos gestionados y las estaciones gestoras.

Protocolo SNMP (Protocolo Simple de Gestión de Red), se caracteriza por ser un estándar reconocido y tener una gran cantidad de herramientas adicionalmente está presente en cualquier dispositivo de red, este protocolo se encuentra basado en solicitudes de respuestas (GET/SET), GET se usa para monitoreo, identificadores de objetos (OIDs), claves para identificar dados en las respuestas, utilización de Base de Información de Gestión (MIBs), entre las principales estadísticas que genera este protocolo son:

- Bytes Adentro/Fuera (I/O) por una interfaz, errores

- Carga de CPU
- Tiempo arriba (*"Uptime"*)
- Temperatura u otros OIDs específicos

Datos por clientes (Servidores o dispositivos clientes):

- Espacio en disco duro
- Software instalados
- Procesos Corriendo
- Entre otros

Este protocolo utiliza un servicio no orientado a la conexión UDP a través del puerto 161, datos de las diferentes versiones:

- v1 implementada en 1988, RFC1155, RFC1156, RFC1157, Especificaciones originales.
- v2 maneja nuevos tipos de datos, metodología de recopilación de datos mejorados (GETBULK), la versión más usada es v2c la desventaja es que carece de método de alta seguridad), RFC1901…..RFC1908+RFC2578.
- V3 la diferencia es que maneja métodos de alta seguridad RFC3411….RFC3418.

Entre los principales roles de SNMP se menciona que la entidad gestora, recopila y presenta la información de los dispositivos y servidores, el dispositivo gestionado contiene un agente de gestión que responde a las encuestas de la entidad gestora.

Comandos Básicos.

Tabla 8 Comandos Básicos

GET	Entidad Gestora - agente
	Solicitud de valor variable único
GET-NEXT	Entidad Gestora - agente
	Solicitud valor siguiente (recursivo, para listas)
GET-RESPONSE	Agente-entidad gestora
	Respuesta a GET/SET, o error
SET	Entidad Gestora - agente
	Configura un valor, o ejecutar acción
TRAP	Agente-entidad gestora
	Notifica espontáneamente de incidente (falla de línea, temperatura por encima de límite, etc.)

2.3.1.2 ADMINISTRAR Y CONTROLAR LOS RECURSOS DE UNA RED

Es el conjunto de reglas que facilitan el mantener una red operativa, eficiente y segura, generalmente nos proporciona la facultad de monitoreo contante, entre los principales objetivos del control de red se encuentra la posibilidad de tener mejoras continuas lo que deberá general una mejor resolución de problemas y una mejor administración de recursos, otro punto muy importante es hacer que la red sea más segura, impidiendo accesos no autorizados, haciendo imposibles que personas ajenas puedan acceder a la información que se genera en ella, finalmente deberá realizar un control de cambios y actualizaciones en la red que afecte en un ínfimo nivel el servicio de los usuarios de red.

El uso de distintos tipos de tecnologías de servició de conectividad como lo son Vsat, Fibra Óptica y ADSL así como el empleo de distintos sistemas operativos como lo son Windows y Linux da como resultado que la administración y control de red sea más importante y compleja.

2.3.1.3 PLANIFICAR LOS RECURSOS DE UNA RED

Para poder cumplir con el objetivo de los infocentros es necesario considerar los siguientes parámetros en cuanto a recursos de red se refiere:

Computadores Personales: la cantidad utilizada de recursos RAM, CPU y almacenamiento en disco duro; frecuencia de uso de aplicaciones.

Capacidad del servidor: La capacidad del servidor puede variar en función del tipo y número de usuarios, la configuración del servidor y la red. El servidor debe cumplir los requisitos del sistema.

- Demanda de los usuarios: La cantidad de RAM y CPU que los usuarios del servidor necesitan depende de las aplicaciones que usan, la frecuencia con la que usan las aplicaciones y la cantidad de trabajo que realizan en un tiempo determinado.
- Requisitos de las aplicaciones: Comprobar los requisitos del sistema de cada aplicación que se tiene pensado instalar en el servidor. Considerando que los requisitos de RAM y CPU aumentan en función de la cantidad de sesiones de usuario que se espera ejecutar simultáneamente.

Características del Router Wireless: Para la implementación de un infocentro se utilizará un Router wireless, estándar 802.11.

El Router interconectará redes inalámbricas (WLAN) y permitiendo proveer servicios a los equipos para que hagan la petición.

También permitirá determinar caminos alternos para que los datos fluyan de manera más eficiente en la red WLAN.

La señal que llega hasta cada infocentro puede llegar por diferentes medios:

- Fibra Óptica
- Radio Enlace
- Comunicación Satelital

Características de las PC: Cada PC tiene una memoria RAM que soporte las aplicaciones escritas previamente en los acuerdos de nivel de servicio, Tarjeta de red inalámbrica compatible con el estándar 802.11 y que cumpla la certificación WI FI.

Características de la impresora: Inalámbricas, de inyección a tinta, multifuncional.

2.3.1.4 COORDINAR LOS RECURSOS DE UNA RED

Se establece la necesidad de una administración de los recursos de la red, en los que se prioriza la reducción de costos y mejorar la eficiencia. De acuerdo a esto se deberá considerar el equipamiento, servicios y personal, que son las partes esenciales y básicas.

La implementación de directrices adecuadas para la gestión de los recursos permitirá un mejor desempeño y establecerá parámetros apropiados para la coordinación. Pasar del que hacer al cómo hacerlo.

Utilizar una documentación adecuada en todos los aspectos ayuda a implementar mejores servicios con mejoras en la infraestructura.

- **Perspectiva del Ministerio de Telecomunicaciones y Sociedad de la Información**

Se debe determinar con exactitud los requerimientos del Ministerio en lo referente a los servicios y necesidades con proyección a mejoras en la ampliación de la red de infocentros.

La utilización de procesos que es un conjunto de actividades que se los puede dividir en tareas es esencial para construir un estándar en la implementación de un servicio, con lo que se puede reducir el costo.

- **Coordinación de la infraestructura**

Coordinar todos los elementos que conforman la infraestructura de la red. Desde los elementos, su interconexión, los entornos distribuidos como son Cliente /Servidor y servicios adicionales proporcionados.

Se debe estipular los SLA (Acuerdos de Nivel de Servicio) con los proveedores y al mismo tiempo estipular los SLO (Objetivos de Nivel de Servicio) para llegar a acuerdos necesarios en la implementación de equipos y servicios. Esto establece parámetros para el correcto funcionamiento de la red de infocentros.

El análisis previo de los lugares a implementar tiene como consecuencia una calendarización exacta de las implementaciones y fiscalizaciones, esto conlleva a una reducción de horas hombre y ayuda a la ejecución rápida y eficaz.

- **Coordinación de Servicios**

Se considera algunos aspectos relacionados con los servicios como: asegurar que esté disponible para los usuarios finales, control o administración en la fase de desarrollo, asegurar la transmisión de información y verificar su correcto almacenamiento. Esto contribuye el correcto monitoreo de esta manera lograr establecer fallas en el sistema.

Los datos obtenidos generan información valiosa sobre la condición del proyecto y tomar medidas correctivas si ese fuera el caso o ratificar acciones que dieron buenos resultados.

En este campo se establece una serie de recomendaciones en la administración de sucesos que pueden aparecer en los servicios.

- Incidentes
- Configuración
- Cambio
- Terminación

} Soporte del Servicio

- Nivel de Servicio
- Financiero
- Capacidad
- Disponibilidad
- Continuidad

} Entrega del Servicio

La coordinación de servicios es una parte fundamental ya que abarca la idea de lo que desea el Ministerio ofrecer y recibir.

- **Coordinación de Personal**

Establecer las capacidades del personal para ubicarlos en un determinado puesto da como resultado un mejor rendimiento y un mejor ambiente laboral. Se consideran ciertos aspectos con lo cual se puede establecer métodos de control y verificar la funcionalidad de un proceso ejecutado.

Establecer un sistema válido para la coordinación de personal, ayuda a la mejora continua con la capacitación adecuada, estableciendo cursos y evaluaciones calendarizadas.

2.3.1.5 ASIGNAR LOS RECURSOS DE UNA RED

Se pueden asignar más recursos a un medio donde el tráfico de la red es más pesado o al distribuir los medios de red para que los recursos de acuerdo a las necesidades reales, con lo cual se aumenta la eficiencia del sistema para procesar paquetes. La gestión de recursos de red es útil para las siguientes tareas:

- Suministro de red.
- Establecimiento de acuerdos de nivel de servicio.
- Diagnóstico de problemas de seguridad.

Asignación de los siguientes recursos:

- Asignar Hardware (Equipos, tarjetas de interfaz, servidores, routers, cableado)

- Asignar recursos Logísticos (SO Libre, Aplicaciones)
- Asignar conexión (Ancho de Banda, Fibra óptica, satelital, radioenlace)

RECURSOS BASADOS EN LA CANTIDAD DE USUARIOS

La asignación de recursos está basada en la cantidad de usuarios de Infocentros, en el nivel de conocimientos y la locación del mismo, dependiendo de la población o tamaño, que permitirán una mejor gestión de usuarios.

Los sistemas operativos de red permitirán al administrador de la red determinar las personas, o grupos de personas, que tendrán la posibilidad de acceder a los recursos de la red. El administrador de una red puede utilizar el Sistema Operativo de Red para:

- Crear permisos de usuario, controlados por el sistema operativo de red, que indican quién puede utilizar la red.
- Asignar o denegar permisos de usuario en la red.
- Eliminar usuarios de la lista de usuarios que controla el sistema operativo de red.

Para simplificar la tarea de la gestión de usuarios en una gran red, el sistema operativo de red permite la creación de grupos de usuarios.

Mediante la clasificación de los individuos en grupos, el administrador puede asignar permisos al grupo.

Todos los miembros de un grupo tendrán los mismos permisos, asignados al grupo como una unidad.

Cuando se une a la red un nuevo usuario, el administrador puede asignar el nuevo usuario al grupo apropiado, con sus correspondientes permisos y derechos.

Mediante la agregación de servicios activados dinámicamente, los proveedores de servicios pueden asignar recursos de red para generar ingresos adicionales

GESTIÓN DE LA RED

Algunos sistemas operativos de red avanzados incluyen herramientas de gestión que ayudan a los administradores a evaluar y controlar el comportamiento de la red. Cuando se produce un problema en la red, estas herramientas de gestión permiten detectar síntomas de la presencia del problema. El administrador de la red puede tomar las acciones preventivas o correctivas dadas una supuesta caída de la red.

DERECHO DE USUARIOS Y GRUPO

El administrador de la red le asigna a cada usuario un grupo, y luego puede asignarle derechos encomendados directamente a todo el grupo, por lo que permite la reducción de tiempo al no hacerlo usuario por usuario. Estos derechos también pueden asignarse a grupos de usuarios en forma indirecta, a través de equivalencias. Los derechos se pueden conceder tanto a los usuarios individuales como a los usuarios pertenecientes a un grupo. Esto permite una seguridad en el acceso a archivos y directorios, ya que si el usuario no desea compartir cierta información, lo comunica al administrador y este a su vez restringe el acceso a la información a los demás usuarios.

PLANEACIÓN ESTRATÉGICA

En todos los sistemas de tecnología existen variables para su planeación estratégica ya que debe haber áreas de trabajo para cada una de las funciones que se realizan de entre las cuales podemos mencionar:

Supervisor de red: Puesto más nuevo dentro del área que se trata de administrar, ejecutar y desarrollar las funciones que tiene que ver con las instalaciones de la red.

Área de análisis: Aquí se analizan los problemas de los infocentros para dale una solución sistematizada.

Área de programación: Recibe información del área de análisis para codificar los programas que se van a suministrar al sistema de cómputo.

Área de captura: Lugar en el cual se almacena la información en la computadora para su procesamiento.

Operadores de cómputo: es donde se encuentra el responsable de administrar la consola de sistemas.

PLANEACIÓN DE RECURSOS

En esta etapa de la planeación el jefe, encargado o administrador del centro de cómputo, organiza los recursos económicos con que se cuenta, es decir, destina la cantidad de recursos necesarios para la subsistencia de cada departamento.

Es la manera de organizar al personal de acuerdo a sus capacidades y funciones que se le asignan dentro de su departamento, como se muestra a continuación:

Profesional de tecnología: Persona con los conocimientos más profundos en el campo de la informática, por lo general es el encargado de administrar los centros de cómputo.

Supervisor de red: Persona capaz de administrar, supervisar y desarrollar las aplicaciones y el mantenimiento de la red.

Analista de sistemas: Persona capacitada para analizar y solucionar los problemas o percances que se generen dentro del proyecto, elaborando para su desempeño (algoritmos, diagramas de flujo) y otros recursos del analista.

Programador: Persona con amplios criterios y conocimientos en programación, con los cuales desarrolla y programa las computadoras del infocentro.

Capturista de datos: responsable de alimentar la información al sistema de cómputo, sus capacidades deben ser (velocidad en el uso del teclado, uso de procesador de texto, hojas de cálculo, bases de datos y paquetería en general.

Operador de computadora: Persona con amplios criterios que usa el sistema operativo y opera todos sus sistemas.

2.3.1.6 MONITORIZAR LOS RECURSOS DE UNA RED

El monitoreo de una red de comunicaciones en los infocentros permitirá detectar y notificar oportunamente eventualidades de red, también muestra el comportamiento de equipos instalados, para esto se utiliza herramientas tecnológicas remotas que se basan en parámetros como análisis y recolección de tráfico de red.

Esta herramienta permite brindar un mejor servicio a los usuarios de la red Infocentros, ya que envía alarmas en caso de degradación de la señal del servicio de internet, para cumplir con estándares de calidad de servicio en el acceso a la información.

La herramienta utilizada es software desarrollado para monitorear dispositivos y aplicaciones en tiempo real, muestra el comportamiento del tráfico de red, la utilización de los recursos y servicios web.

Las principales características que se van monitorear en nuestra red son las siguientes:

Monitoreo de configuración

- Control de equipamiento físico
- Procesos de modificación, backup y restauración de configuraciones de red.

- Monitoreo de recursos claves para alertas, Reparación de fallos

Monitoreo de desempeño

- Busca cuellos de botella o problemas de congestión de la red.
- Problemas sistemáticos de performance.
- Planificación de Capacidad

Monitoreo de seguridad

- Actividades para controlar medidas de seguridad en la red.

Monitoreo de cuentas

- Actividades para contabilizar quien utiliza los servicios de red por medio de perfiles de usuarios creados.
- La utilización del protocolo SNMP (Simple Network Protocol Manager), que permite visualizar datos como utilización de ancho de banda en los enlaces, consumo de CPU en switchs y routers, alarmas de conexión física, lógica y de procesamientos.
- Para la elección de la herramienta óptima de monitoreo que cumpla con los requerimientos del Ministerio de Telecomunicaciones y Sociedad de la Información deben ser: Perfil de personal de administración, sistema operativo Software libre, recursos económicos, Equipos instalados y sus características.

El propósito fundamental del monitoreo es la recolección de información de funcionamiento de las distintas capas en la comunicación, recepción y procesamiento de alarmas de red.

2.3.2 GESTIÓN DE RED - COMPONENTES

2.3.2.1 GESTIÓN DE CONFIGURACIONES/CAMBIOS

Mantener información sobre el diseño de la red

Se debe definir los elementos a gestionar, llevar un registro de configuraciones de red actualizado, hacer revisiones rutinarias en caso de cambios realizados, basado en parámetros de tiempo o cambios de configuración y topología inminentes en nuestra red.

En cuanto al manejo de configuración de software se debe tener en cuenta:

- Ejecutables
- Modelos de procesos
- Modelos de datos
- Especificaciones de requisitos
- Código fuente
- Pruebas realizadas

De estas configuraciones en la documentación debe estar presente:

- Nombre
- Versión
- Estado
- Localización

Los componentes o elementos de la red se dividen por sus características puedes ser fijos o dinámicos.

FIJOS

Elementos de configuración:

Son componentes de la infraestructura IT, que se encuentran configurados dentro de la organización, permite tener un concepto claro de su función en cada departamento y permite actualizar corregir, verificar y controlar errores remotamente en la red.

Hardware

Servidores, Thin Clients PCs, Impresoras, Routers, Monitores y sus componentes como lo son:

- Mouse
- Teclado
- Tarjetas de red

Software

Sistemas operativos, Aplicaciones y Protocolos de red.

Documentación

Hojas de especificaciones técnicas, Manuales del usuario y Acuerdos de niveles de servicio.

Ubicación de elementos instalados, lugar exacto Provincia, Ciudad, Cantón, parroquia Comunidad o asociación en donde prestan sus funciones los equipos de red.

Cómo está conectado, cuál es su característica de conexión y desempeño dentro de la estructura de la red.

Diagrama de red, se refiere a tener diagramas de fácil interpretación por las personas técnicas, en caso de soporte a todo nivel.

Responsable de los elementos de red, se refiere a los administradores de la red encargados de supervisar las funcionalidades de los equipos instalados, respaldar la información y obtener respaldo de configuraciones de los dispositivos administrables.

Comunicación con los responsables, se debe tener un lazo de comunicación constante entre los usuarios, gestores y administradores de la red, para un mejor desempeño de los recursos de red

DINÁMICO

Estado de conexión de cada dispositivo de infraestructura, se refiere a la disponibilidad de los elementos de la red, saber su estado físico y lógico.

Es el proceso que permite identificar los elementos de red, controla el cambio en cada uno de ellos a lo largo de su vida útil. Así, entre los elementos de configuración, se encuentran no únicamente ejecutables y código fuente, sino también los modelos de datos, modelos de procesos, especificaciones de requisitos, pruebas, etc.

En resumen, todos los componentes que han de ser gestionados.

Gestión de inventario

Base de Datos de la Gestión de Configuraciones, llamada CMDB no se limita a enumerar el stock de elementos, dispositivos sino que nos brinda una imagen global de la infraestructura TI de la organización**:** esta base de datos debe incluir:

- Información detallada de cada elemento de configuración.
- Interrelaciones entre los diferentes elemento de configuración, como, por ejemplo, relaciones "padre (servidor)-hijo (thin Client)" o interdependencias tanto lógicas como físicas.

Gestión de Red

- Gestión de configuraciones
- Gestión de inventario
- Base de datos de elementos de la red
- Historia de cambios y problemas
- Mantenimiento de Directorios
- Todos los nodos y sus aplicaciones
- Base de datos de nombres de dominio
- Gestión de proveedores externos

- Gestión de configuraciones
- Gestión de SLAs (*"Service Level Agreements"*):
- Contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas
- Identificación de las partes contractuales
- Identificación del trabajo a realizar
- Objetivos de niveles de servicio
- Niveles de servicio proporcionados
- Multas por incumplimiento
- Fecha de caducidad
- Cláusulas de renegociación
- Prestaciones actuales proporcionadas
- Gestión de configuraciones
- Gestión de incidencias: TTS
- Fecha/Hora de prestación servicios
- Informe de incidencia
- Resolución de incidencia
- Usuario/localización
- Equipo afectado
- Descripción del problema
- Operador/es
- Grado de severidad
- Historial de incidencia
- Comentarios

2.3.2.2 GESTIÓN DEL DESEMPEÑO/CONTABILIDAD

Se debe realizar un sistema de control interno distribuido en grupos, que dependen del número de equipos instalados y condiciones de red para detectar abusos o distribuciones desequilibradas de los recursos de red.

Mediante herramientas de medición se contabiliza las personas que utilizan los recursos de red, y sus respectivas aplicaciones.

Las principales tareas que debemos buscar para mantener nuestra red de forma eficiente y cumplir un buen desempeño es la distribución de recursos tomando en cuenta los siguientes parámetros:

Identificación de equipos instalados, se refiere a conocer que equipos se encuentran conectados en nuestra red conocer su marca, modelo, serie entre otras características que debemos conocer en detalle, para llevar un control de bienes o definir un inventario.

Establecer políticas de tarifación, se refiere conocer tablas de valores económicos por concepto a servicio de tecnología, para cobrar por los servicios a nuestros usuarios y pagar a nuestros proveedores.

Definición de procedimientos para tarifación, se refiere a definir parámetros en tiempos y formas de pago para la socialización a nuestros potenciales usuarios.

RADIUS/TACACS:

Mediante este servidor se contabiliza las personas que acceden a los servicios de forma alámbrica e inalámbrica, mide estadísticas de interfaces y estadísticas de protocolos utilizados.

Los recursos que puedes ser sujetos a monitorización mediante herramientas de gestión por ejemplo:

NETFLOW (CFLOWD, FLOW-TOOLS, FLOWSCAN):

Mediante estas herramientas que reúnen y presentas información de flujos de tráfico, información acerca de direcciones, puerto de origen y destino, que servirán para la contabilidad y estadística del desempeño de nuestra red.

Está destinado a personas que pertenezcan a sectores jurídicamente establecidos, que necesiten acceder servicios de tecnologías de la información, deben cumplir requisitos mínimos como:

- Infraestructura civil disponible
- Energía eléctrica disponible
- Libre acceso a personas del sector

Seguridades físicas en sitio

2.3.2.3 GESTIÓN DE FALLAS.

En los distintos escenarios se puede establecer fallas en los componentes de la red, los cuales pueden provocar que los servicios sufran de intermitencia o que dejen de funcionar, por tal motivo es necesario una gestión de los sucesos que ocurran y que pueden provocar un declive de la red. Así se puede mejorar el performance y reconocer las fallas, corregirlas en un menor tiempo e identificar posibles problemas.

Se puede realizar dos tipos de gestión de fallas, la primera es reactiva, es decir cuando la falla ocurre y se la analiza para descubrir por qué y proponer soluciones. La segunda es

conocida como proactiva esta se refiere exclusivamente a realizar un monitoreo constante y verificar la calidad de los servicios de la red, con el objetivo de prevenir futuras fallas.

El objetivo principal de la gestión de fallas es el restablecimiento de los servicios, no se centra en el conocer cuáles fueron las causas u orígenes de los problemas. Solo cuando el incidente es recurrente o genera un mayor impacto a la red es necesario que se investigue el origen o las causas.

Dentro de esta gestión se puede considerar los siguientes aspectos:

- La estructura total de la red
- Detectar cualquier falla en los servicios.
- Registrar y clasificar las fallas.
- Asignar el personal encargado de restaurar el servicio al verificar los acuerdos de nivel de servicio establecidos en un contrato.

El conocimiento total de la red es primordial ya que se puede comprender de mejor manera los equipos que provocan una determinada falla en los servicios.

Mediante los sistemas de gestión de red se puede detectar los problemas, de forma que se lleve un registro total y se pueda clasificar; esto genera estadísticas claras de las fallas, con la finalidad de crear procesos eficaces y rápidos para solventar problemas.

La clasificación establece la priorización de las fallas al utilizar dos parámetros:

- Impacto, establece la afectación que provoca la falla.
- Urgencia, establece el tiempo en el que la falla debe ser resulta de acuerdo a los SLA.

Previo a la asignación del personal para que solucione un determinado incidente es necesario hacer un diagnóstico que permita la rápida identificación de los elementos involucrados, establecer en donde se originó el problema y corregirlos de la forma más rápida y eficaz.

De acuerdo a la priorización de las fallas es posible realizar un escalamiento adecuado para la resolución del problema, desde un primer nivel de soporte que solo involucre ayuda no física como llamadas telefónicas o mensajes, hasta involucrar la movilización de personal y recursos.

La solución de incidentes es prioritaria si afecta a uno o más servicios, por lo que es necesario que se lleve un registro adecuado de los procedimientos para dar solución, esto permitirá que los problemas futuros se resuelvan de una forma rápida.

Al final se debe cerrar el incidente, pero se debe verificar con los usuarios que los servicios se encuentran sin novedad y funcionales en su totalidad.

2.3.2.4 GESTIÓN DE SEGURIDAD

En la red de infocentros, uno de los aspectos fundamentales y tal vez el más importante es la información, asegurar que llegue a su destino de forma íntegra, confiable y disponible son las características indispensables que hacen de un sistema óptimo.

En la actualidad la vulnerabilidad de los sistemas es visible ya que son constantemente son atacadas por virus o la información es robada o alterada, en sistemas en los que los datos son primordiales es necesaria una encriptación (no es el caso de la red de infocentros).

Por tal motivo los sistemas que brinden seguridad deben sustentarse en tres conceptos:

Confidencialidad, debe asegurar que la información sea destinada solo a las personas que deben tener acceso a esta, asegurando que no pueda ser vista por personas ajenas y que hagan mal uso de ésta.

Integridad, es primordial que la información no sufra de alteraciones las que pueden generar datos no verídicos. Se utiliza sistemas de encriptación los que pueden ser más o menos robustos dependiendo de la prioridad de la información.

Disponibilidad, la información debe estar accesible todo el tiempo.

Al diseñar una política adecuada de seguridad hay que establecer una colaboración con los usuarios y administradores todo esto en función del provenir del proyecto, esto se lograra mediante el cumplimiento de los acuerdos firmados y siempre tratar de minimizar los riesgos.

La seguridad de los datos de la red no es de uso exclusivo de las personas que son expertas en seguridad, hay que tener en consideración que todos los miembros de la parte administrativa del proyecto son responsables de la información ya sea en mayor o menor medida, pero se debe establecer que una falla por más mínima que sea puede provocar el declive.

Es indispensable que se cree políticas de seguridad, en las que se establezca objetivos, responsabilidad y los recursos. Las políticas de seguridad deben estar de acuerdo con la funcionalidad de la red, coordinar los procesos, verificar protocolos de acceso a la información, el tipo de monitorización que se va a llevar a cabo, los informes que deben ser presentados, el plan de seguridad y recursos de software y hardware.

Una parte fundamental de este plan de seguridad es la parte humana, la cual es la más vulnerable y por tal motivo es la que debe ser considerada con más profundidad. En este caso establecer los procesos y procedimientos, quienes son los responsables del proceso de gestión, de los subprocesos.

El plan de seguridad debe establecer parámetros desde el inicio y ser suscritos en los acuerdos de nivel de servicio, en los acuerdos de nivel de operación y en los acuerdos de soporte. Los expertos deben establecer pasos a seguir en el caso que los incidentes no consten en el plan de seguridad que se estableció en los acuerdos de servicio, con esto se puede solventar problemas inesperados.

Se debe establecer que el plan de seguridad no debe estar diseñado de tal forma que restrinja la operación.

La aplicación de las medidas de seguridad es esencial ya que si no se lo hace de nada sirve establecer un plan con anterioridad.

La parte vulnerable de la seguridad es el ser humano, se considera los siguientes aspectos para establecer reglas claras con el personal:

- El personal acepta y conoce las medidas de seguridad y las responsabilidades que poseen.
- La firma de acuerdos de responsabilidad correspondiente a su cargo.

La información debe ser entregada con anticipación al personal para que se prevea de posibles fallas por falta de esta.

Se establece líneas de seguridad propias de la gestión de seguridad:

- Asignar los recursos necesarios para la gestión en sus distintos niveles.
- Documentar y archivar la información necesaria.
- Instalar y mantener las herramientas necesarias para garantizar la seguridad.
- Establecer como prioridad los cambios de versiones para evitar la aparición de nuevas vulnerabilidades.
- Establecer políticas y protocolos en todos los niveles para el acceso de la información.
- La monitorización debe ser una herramienta fundamental para detectar ataques o intrusiones.

EVALUACIÓN

Una correcta medida de la gestión de seguridad es la evaluación, se debe dar cumplimiento de las medidas de seguridad por tal motivo se las debe evaluar, verificar sus resultados y establecer si se dio cumplimiento a los acuerdos de nivel de servicio.

La evaluación debe ser interna pero de ser el caso se puede establecer la utilización de auditores externos los cuales establezcan resultados de forma imparcial, de forma que puedan proponer mejoras, todo esto con la debida documentación.

Se establece que las evaluaciones son periódicas pero en el caso de que se presenten incidentes que afecten de gravedad a los infocentros, se debe realizar una auditoría para conocer los detalles.

MANTENIMIENTO

Se debe mantener las reglas de seguridad cuando estas se encuentren funcionales y actualizadas, la falsa sensación de seguridad debida a reglas obsoletas puede provocar fallas graves para la red.

La actualización de las reglas es una parte fundamental del mantenimiento y prevé futuros peligros. En esta actualización debe ingresar tanto el software como el hardware y sin olvidar la parte humana que es la parte más vulnerable.

2.3.2.5 SEGURIDAD EN EL TRANSPORTE DE LOS DATOS

La seguridad de las redes y las comunicaciones debe cumplir con algunas necesidades.

- Número de vulnerabilidades descubiertas.
- Número de rupturas *("breaches")* de cortafuegos.

La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.

- Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de uso final.
- Número de incidentes que impliquen dispositivos de uso final.
- Número de dispositivos de uso final no autorizados detectados en la red o en el entorno.

Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con los roles en el negocio.

- Promedio de tiempo entre cambios y actualizaciones de cuentas.
- Numero de cuentas (con respecto al número de usuarios/ funcionarios autorizados)

2.3.2.6 MECANISMOS DE SEGURIDAD

Se deben implementar medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.

- Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno.
- Clasificación medida para las evaluaciones de seguridad física.
- Número de incidentes relacionados con seguridad física.

La información electrónica debe tener medidas apropiadas mientras está almacenada.

- Número de incidentes relacionados con accesos no autorizados a la información.

Proteger la información contra software malicioso (malware). Implementar y mantener medidas efectivas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo del proyecto de infocentros para proteger los sistemas de la información y tecnología del software malicioso (por ejemplo virus, gusanos, software espía -"*spware*"- y correo basura).

- Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.
- Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera.
- Distribuir todo el software de protección de forma centralizada, usando una configuración centralizada y la gestión de cambios.
- Revisar y evaluar regularmente la información sobre nuevas posibles amenazas.
- Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a la información no solicitada.
- Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.

Gestionar la seguridad de la Red y las conexiones. Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

- Basándose en el análisis de riesgos y en los requerimientos del negocio, al estableces y mantener una política de seguridad para las conexiones.
- Permitir solo a los dispositivos autorizados tener acceso a la información y a la red. Configurar estos dispositivos para forzarla solicitud de contraseña.
- Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
- Cifrar la información en tránsito de acuerdo con su clasificación.
- Aplicar los protocolos de seguridad aprobados a la conexión de red.
- Configurar los equipos de red en forma segura.
- Estableces mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
- Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
- Realizar pruebas periódicas de seguridad del sistema para determinar la adecuación de la protección del sistema.

Gestionar la seguridad de los puestos de usuario final. Asegurar que los puestos de usuario final (es decir portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) está asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.

- Configurar los sistemas operativos de forma segura.
- Implementar mecanismos de bloqueo de los dispositivos.
- Cifrar la información almacenada de acuerdo a su clasificación.
- Gestionar el acceso y control remoto.
- Gestionar la configuración de la red de forma segura.
- Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
- Proteger la integridad del sistema.
- Proveer de protección física a los dispositivos de usuario final.
- Proteger la integridad del sistema.
- Proveer de protección física a los dispositivos de usuario final.
- Deshacerse de los dispositivos de usuario final de forma segura.

Gestionar la identidad del usuario y del acceso lógico. Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de los infocentros.

- Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad.
- Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación).
- Segregar y gestionar cuentas de usuario privilegiadas.
- Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.

- Asegurarse que todos los usuarios (internos, externos y temporales) y su actividad en sistemas TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente.

Supervisar la infraestructura para detectar eventos relacionados con la seguridad. Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

- Registrar eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
- Definir, comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.
- Revisar regularmente los registros de eventos para detectar incidentes potenciales.
- Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciando de los requerimientos.
- Asegurar que todos los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

CAPÍTULO III:

ANÁLISIS TÉCNICOS DE REQUERIMIENTO

3.1. ALCANCE TÉCNICO.

Se busca definir el diseño de una solución integral para la implementación de un centro integrado para la gestión, control y monitoreo de la infraestructura tecnológica.

3.2. REQUERIMIENTO GENERALES.

El diseño deberá estar alineada a los siguientes procesos de la Biblioteca de la Infraestructura de las Tecnologías de Información (ITIL): EV: Administración de Eventos, IM: Administración de incidentes, KM: Administración del Conocimiento, SACM Administración de Servicios y Configuraciones, SCM Inventario del Catálogo de Servicios registrado, SLM Información para Control de Cumplimiento de los Niveles de Servicio.

La solución debe cumplir con lo siguiente:

- Criterios de flexibilidad, escalabilidad, redundancia, alta disponibilidad, además debe contar con medidas de contingencia que permitan asegurar la continuidad del servicio y la recuperación de desastres.
- Funcionalidades que faciliten la gestión de inventarios de hardware y software, control remoto, registro de cambios y configuraciones, registro de eventos, gestión de incidentes, gestión de activos y herramientas de monitoreo tanto pasivo como proactivo de las plataformas.
- Gestión de hardware, se requiere llevar un inventario del equipamiento informático, como:
    - Tipo de procesador.

- Velocidad de procesador.
- Capacidad de discos duros.
- Capacidad RAM.

- En cuanto al software se requiere el inventario del software instalado teniendo en cuenta las versiones y licencias.

Todo el software incluido en la solución requiere la instalación y configuración para garantizar la compatibilidad e interoperabilidad del sistema.

El sistema debe permitir establecer parámetros de configuración de umbrales de operatividad, correlación de eventos y definición de al menos 3 mapas de servicio.

Se incluirá la configuración, descubrimiento y población de la CMDB para el equipamiento del Core Tecnológico con sus aplicativos e infraestructura relacionada.

Los requerimientos de hardware y software, deberá incluir mínimo 10 licencias nombradas para las siguientes funcionalidades: "*Service Desk*" (Incidentes y Problemas), "*Change*" (Gestión de Cambios), "*Asset*" (Gestión de Activos), *"Service Level*" (Gestión de SLAs), utilizando estándares para su funcionamiento.

Monitoreo de infraestructura tecnológica y servicio de conectividad de 781 infocentros, gestión de despliegue de software en inventario de 8267 estaciones de trabajo que se encuentran en estos infocentros.

Se debe prestar el servicio en la modalidad de "*hosting*" dedicado o "*cloud*" de manera que se garantice su crecimiento en componentes de infraestructura tecnológica.

El sistema deberá suministrar el procesamiento, almacenamiento, respaldo y seguridad informática para ejecutar las aplicaciones del sistema.

Implementar y documentar políticas de seguridad informática para soportar los procesos de administración y monitoreo.

El diseño proveerá la facultad de implementar y probar un plan de recuperación de desastres, el cual debe ser documentado y dará la posibilidad de realizar simulacros.

3.3. MONITOREO PROACTIVO

Se requiere una solución integral de monitoreo proactivo, que controle disponibilidad, performance, usabilidad de recursos y tiempo de respuesta de la infraestructura de TI de la red de telecomunicaciones y de los servicios brindados.

El sistema deberá monitorear servidores físicos y virtuales, bases de datos, aplicativos, web servers, sistemas de mail, dispositivos de red, "*firewalls*" y "*load balancers*", que formen parte de la solución de la infraestructura a ser proporcionada.

El sistema deberá permitir las siguientes facultades:

- Almacenar las métricas monitoreadas durante al menos 6 meses y generar gráficos y reportes personalizables.
- Monitorear la disponibilidad y el tiempo de respuesta de procesos que utilicen protocolos y servicios estándares de red como: DNS, DHCP, SMTP, HTTP, HTTPS, IMAP, POP3, FTP, entre otros.
- Las consolas de operación con interface web.
- Presentar estadísticas de los servicios de TI que se ofrecen a los usuarios Institucionales, las métricas y KPIs que definen la salud del servicio y los elementos de TI y de la red de comunicaciones que lo componen.

- Las métricas comunes o habituales deben estar predefinidas nativamente en la solución y deben ser fácilmente expandibles para incluir nuevas métricas a monitorear.
- Establecer los rangos de comportamiento normal, de alerta y crítico de todas las métricas monitoreadas, tanto sean métricas monitoreadas en forma nativa por la solución o sean métricas predictivas definidas a posterioridad. A este comportamiento normal se lo definirá como parámetros de referencia o línea base.
- Los sensores o módulos de monitoreo deberán registrar el comportamiento de las métricas durante los distintos momentos del día y los distintos días de la semana, con al menos una granularidad horaria.
- Deberá generar alertas, notificaciones y eventos a través de umbrales definidos previamente y realizar notificaciones basadas en la frecuencia de repetición de los eventos registrados, en un período de tiempo o como combinación de ambos. Esta herramienta deberá ser nativamente integrada (mismo fabricante) con la Mesa de Servicios para la creación de tickets generados en forma manual o automática en función de eventos ocurridos.
- Los sensores o módulos de monitoreo deben tener al menos 3 estados. Ejemplo: Normal, Alerta y Crítico.
- La solución deberá generar alertas predictivas, mediante el uso de los algoritmos estadísticos y los umbrales predefinidos, tanto superiores como inferiores, identificando tendencias de problemas en el rendimiento de la infraestructura de TI y/o de la red de telecomunicaciones monitoreada. Esto implica que a pesar de que las métricas no superan los umbrales definidos, se observa una tendencia que

puede indicar un problema en próximos intervalos de tiempo, definidos en el módulo predictivo.

- Generar alertas de tendencias en el comportamiento, para lo cual se requiere el establecimiento de umbrales, los cuales mediante políticas generales o por medio de operaciones masivas, el sistema de monitoreo debe reportar que una métrica está fuera del rango normal de operación, tanto sea por encima o por debajo. Debe hacerlo en forma selectiva para las métricas monitoreadas.
- Ante alertas de tendencias en el comportamiento de la infraestructura y servicio monitoreado, deberá poder ejecutar acciones correctivas, previamente configuradas (Ejemplo: realizar un "*restart*" de proceso automáticamente).
- Ante alertas o eventos debe poder notificar a personas o grupos de personas a través de un mensaje de correo electrónico o un SMS opcional, manejando niveles de escalamiento.
- Ante alertas o eventos debe poder notificar a personas o grupos de personas a través de un mensaje de correo electrónico o un SMS opcional, manejando niveles de escalamiento.
- Proveer facilidades de análisis de causa raíz, ante la caída o degradación del performance de un servicio o elemento TI, debe correlacionar las métricas y eventos existentes para determinar el posible componente de infraestructura que origina la falla.
- Control de acceso para los usuarios. Debe poder definir a que grupos lógicos puede acceder cada usuario y que acciones puede realizar.
- Soportar varios métodos de monitoreo, como: SNMP, v1,v2,v3; JMX, WMI, SQL Query, etc.

- Definir correlación de eventos en cascada para las alarmas, para suprimir falsos positivos. Ejemplo: Si un Web server no responde al comando ping, todas las alertas de transacciones Web de ese web server, deben ser escondidas.
- Se podrá representar cualquiera de los parámetros monitoreados mediante gráficos desde la consola Web.
- Agrupaciones lógicas de los elementos monitoreados y la definición de funciones o servicios virtuales a los cuales se les pueda dar niveles de importancia o pesos que permitan cuantificar el impacto o la afectación de los servicios en cada uno de los eventos.

3.4. MONITOREO DE INFRAESTRUCTURA TECNOLÓGICA

Se deberá incluir la capacidad para el monitoreo de todos los componentes de la infraestructura tecnológica, teniendo en cuenta el equipamiento y las redes de telecomunicaciones que forman, de deberá poder cargar la información sobre los mismos en la CMDB en base al descubrimiento automático realizado con las herramientas incluidas en la solución propuesta.

Las métricas posteriores deberán poder ser usadas por la solución con las mismas capacidades que las métricas pre-existentes. Es decir, debe guardar un historial, mostrar gráficos sobre las mismas, definir umbrales, utilizarlas para el análisis de causa raíz, generar gráficos, reportes.

Deberán poder usar modelos genéricos ("*templates*") para aplicar a nuevos dispositivos o elementos a monitorear.

Deberá utilizar umbrales configurables sobre módulos predictivos, los mismos que en base a la información recopilada en un período de tiempo, puedan predecir el comportamiento futuro de un ítem configurable.

La herramienta de "*servicedesk*" y monitoreo deben estar integradas nativamente, es decir ser del mismo fabricante.

Deberá soportar SNMP v1, v2 y v3.

3.4.1. CONSOLA DE OPERACIÓN

Tabla 9Consola de Operación

ÍTEM	CARACTERÍSTICA
1	Se debe presentar a través de una interface Web
2	Visualización del estado actual de los elementos monitoreados
3	Visualización y administración de alertas
4	Visualización del comportamiento histórico de las métricas mediante gráficos
5	Consulta de métricas en tiempo real
6	Generación y personalización de reportes
7	Definición y modificación de umbrales
8	Consulta y definición de SLAs
9	Definición de alertas y reglas de notificación
10	Manual de acciones de recuperación de la herramienta
11	Cada usuario debe poder personalizar su consola de operación de forma independiente

3.4.2. MANEJO DE ALERTAS Y EVENTOS

Tabla 10Manejo de Alertas y Eventos.

ÍTEM	CARACTERÍSTICA
1	Visualización de eventos activos y cerrados
2	Registro de la fecha y hora de la alerta
3	Elemento afectado y evento generado
4	Diferenciación del estado de la alerta: activa, cerrada, trabajando, etc.
5	Configuración de criticidad de los estados (normal, alerta, crítico)
6	Debe permitir identificar alertas que estén asociadas al evento correspondiente
7	Debe permitir marcar un evento de tal forma que indique que se está trabajando en él
8	Debe permitir asociar comentarios al evento por parte de los operadores

3.4.3. VISUALIZACIÓN DE GRÁFICOS DE MONITOREO

Deberá generar gráficos tipo: lineal, área, X-Y, torta y sobre mapas GIS o de red, manejar varios indicadores diferentes en un gráfico (Ej.: % y Tiempo de Respuesta), también representará por medio de iconos los colores y estados de los diferentes componentes que están siendo monitoreados, graficar una métrica junto con sus parámetros de referencia en el mismo gráfico, tanto numéricos como de información textual, así como exportará los datos de los gráficos.

Permitirá agregar textos descriptivos a los gráficos, para su mejor comprensión.

Podrá restringir el gráfico a un sub-periodo de tiempo definido por ventanas o intervalos de tiempo seleccionados.

Tendrá una visión de "Tablero de Control", con los indicadores principales de los componentes y/o servicios monitoreados los mismos que deben ser personalizables.

Cada uno de los indicadores podrá mostrar el estado actual e histórico de las métricas

Los tableros de control deberán actualizar los indicadores de forma automática.

3.4.4. MÉTRICAS DE REFERENCIA

Registrará por medio de plantillas, políticas de administración y operaciones masivas el comportamiento normal, de alerta y crítico de todas las métricas monitoreadas.

Los parámetros de referencia mostrará el comportamiento de las métricas, con al menos una granularidad horaria.

Podrá calcular módulos sintéticos o predictivos en base al comportamiento histórico.

Los módulos sintéticos o predictivos seguirán ajustándose en forma automática con el tiempo, con la evolución de los datos históricos.

Podrá configurar la forma de calcular los módulos o sensores predictivos.

3.4.5. DEFINICIÓN DE UMBRALES

Facultará la definición de umbrales estáticos con valores fijos.

Al definir módulos predictivos mostrará los rangos aceptables. La presentación de los datos y el monitoreo será en intervalos de tiempo definidos.

Al definir módulos sintéticos, permitirá que los valores dentro de rangos de funcionamiento normal, tengan un margen de tolerancia con respecto a la referencia.

Tendrá al menos tres estados de los sensores o módulos Ej.: normal, alerta y, crítico)

3.4.6. ARQUITECTURA Y ADMINISTRACIÓN

Tendrá una arquitectura escalable que permitirá el crecimiento del sistema.

La base de datos tendrá un esquema abierto que permita el acceso de herramientas de generación de reportes.

Permitirá el monitoreo remoto, no necesariamente desde un servidor central.

Incluirá un sistema de firewalls.

La configuración de los agentes de monitoreo será centralizada.

Los puertos de interconexión entre el servidor y los agentes, que se utilizan para realizar control y acceso remoto, podrán ser configurables.

La comunicación entre el servidor y los agentes debe ser encriptada.

3.4.7. SEGURIDAD Y ACCESO

Se debe manejar restricciones de seguridad en el control de acceso en función de los roles.

Debe manejar un control de acceso por usuario.

Debe permitir crear grupos lógicos para el manejo de reglas.

3.4.8. ACUERDOS DE NIVELES DE SERVICIO

Se podrá definir y registrar los SLA en base a las métricas monitoreadas de los componentes de equipamiento y conectividad.

Se podrá definir SLAs en base a los contratos y convenios existentes, tomando como referencia los servicios que puedan ser monitoreados en forma automática.

Se podrá definir niveles porcentuales de cumplimiento, realizar un registro del cumplimiento de los SLA, registro de fecha y duración del incumplimiento del SLA.

3.5. MAPA DE SERVICIO

Permitirá crear mapas geográficos que incluyan los centros a monitorear a partir de la información de la infraestructura cargada en la CMDB, crear un modelo de dependencia de servicios que mapee lógicamente las relaciones entre los servicios y los sub-servicios, creación y visualización de los mapas de servicio.

Permitirá seleccionar cada mapa de servicio y ser escogido en cualquier momento por el usuario para su visualización, aplicando los permisos y los grupos a los que se haya autorizado.

El mapa gráfico de servicio deberá reflejar en tiempo real el estado de los servicios y cada uno de sus componentes empleando un código de colores, cada elemento del mapa de servicio debe mostrar su estado actual y mediante selección, información detallada del

mismo, empleará mapas gráficos que permitan relacionar servicios de TI, localizaciones físicas y niveles de servicio.

Indicará mapas de impacto, que una falla de TI provoca en los servicios en función de intervalos de tiempo predefinidos.

Definirá el modelo de servicio, para identificar de forma rápida que servicios se ven afectados por un determinado problema.

El modelo de servicios debe facilitar la administración de los servicios de TI y de la red de comunicaciones desde una interfaz gráfica.

El modelo de servicios permitirá descubrir de forma rápida el recurso que está siendo monitoreado de equipamiento o de conectividad que causa la interrupción del servicio.

Tendrá interfaz WEB para el acceso y operación de los usuarios y control de autenticación y seguridades de acceso.

Proveerá un entorno gráfico para desarrollar y administrar el modelo de servicios e integración nativa con los sistemas que manejan los procesos de gestión de incidentes y eventos.

Los componentes representarán los recursos de la red de telecomunicaciones que brindan el servicio, como son: aplicativos, servidores, bases de datos y dispositivos de red, recursos lógicos como grupos de usuarios, regiones geográficas y procesos de negocio.

Cuando un componente es afectado por una falla en alguno de los subcomponentes, se deberá resaltar cuál de los subcomponentes es el que lo está originando.

Se podrá definir inter-dependencia entre los componentes.

3.6. MESA DE AYUDA

Asignación automática de un número de caso para las solicitudes de usuarios realizadas vía telefónica, vía mail, o Web en la herramienta de seguimiento y gestión.

Registro de identificación de usuario la primera vez que llama al centro de monitoreo, con la siguiente información: nombre del Infocentro, provincia, cantón, parroquia, dirección, email, teléfono, etc. A partir de la segunda comunicación, con el nombre de usuario, se obtendrá toda la información asociada.

La opción de efectuar encuestas personalizadas para ser enviadas automáticamente al usuario final, en donde se evalúe y reporte la calidad del servicio recibido.

Categorización de las solicitudes de usuario como incidente o requerimiento.

La solución deberá contar con una biblioteca de los eventos reportados con mayor frecuencia por parte de los usuarios, de tal manera que permita la solución de eventos en el primer nivel de soporte, con funcionalidades de mapeo automático según una clasificación determinada. Una vez detectada la solución esta deberá ser relacionada al registro de la llamada (incidente o requerimiento).

El diseño deberá facilitar la integración con la gestión de niveles de servicios, de tal manera que permitan generar las notificaciones automáticas de los eventos de acuerdo su criticidad, ya sean estos requerimientos o incidentes.

Asignación automática de los eventos al operador de Service Desk en base a la carga de trabajo y nivel de soporte.

Configuración de niveles de seguridad, autenticación y acceso al sistema, para el personal operativo o administrativo.

La mesa de ayuda debe tener un nivel de integración inmediato y completo, con los demás componentes de la solución.

Debe incorporar la opción de difusión de comunicados de alerta por correo electrónico a grupos de usuarios, respecto a situaciones que puedan afectarlos.

Se deberá permitir crear y recuperar de manera rápida y eficiente los datos del solicitante, validando su identificación contra la base de personas de la organización.

La diseño debe soportar ser configurada y puesta en producción en una arquitectura de alta disponibilidad.

3.7. GESTIÓN DE INCIDENTES.

Asignación de un ticket ID único de manera automática para el seguimiento del requerimiento desde el primer nivel de soporte hasta su solución.

Registro de la información básica: usuario, problema, hora, categorización del evento, solución.

La herramienta diseñada deberá notificar automáticamente a los usuarios operadores y administradores del sistema implicados cuando se registre una nueva incidencia

Clasificación del incidente por criticidad: bajo, medio, alto, crítico.

Registro del incidente en una base de datos central.

Búsquedas de eventos por cualquier campo de registro.

Se deberá contar con un campo tipo bitácora para registrar la solución del caso. Este campo no debe ser editable una vez guardada la información y debe ser incremental de manera que se vayan agregando entradas a medida que se trabaja sobre el incidente. Debe

quedar registrando usuario, fecha y hora de la actualización, sin posibilidad de eliminar las entradas anteriores.

Se deberá permitir realizar filtro de los eventos por SLAs y tiempo estimado de solución.

Facilidades para que los usuarios finales puedan reportar, modificar y cerrar incidentes a través de la interfaz web.

Registro en un archivo log o en la Base de Datos del acceso de cada uno de los operadores

Categorización del incidente de acuerdo a la afectación, indisponibilidad parcial, intermitencia de servicio, indisponibilidad total.

Gestión de estados del incidente (nuevo, en curso, pendiente por, escalado o cerrado)

Deberá tener un campo en donde se registre la solución definitiva o temporal.

Deberá brindar opciones de asignación automática de incidencias a los grupos correspondientes.

Seguimiento del incidente: (monitoreo, estado, informar al usuario final sobre el estado del incidente)

Registro del cierre del incidente, comunicación al usuario final.

Generación de reportes estadísticos (Mínimo: soportes pendientes, cantidad de soportes atendidos por cada agente, tipo de incidentes, incidentes frecuentes, de servicios solicitados por usuario, incidentes cerrados, etc.).

Reportes parametrizables y exportables a archivos Excel.

Ingreso de parámetros de acuerdo a las políticas que se definan para las diversas disciplinas de gestión.

Debe permitir vincular el ítem de configuración afectado y el servicio afectado por el incidente.

La herramienta diseñada deberá permitir asignar actividades/tareas y hacer el seguimiento de las mismas: persona asignada, estado, inicio, fin.

Se deberá permitir relacionar eventos que tienen un problema raíz en común, la cual debe ser registrada.

3.8. GESTIÓN DE NIVELES DE SERVICIOS.

La herramienta deberá permitir la gestión de los acuerdos de nivel de servicio.

La solución deberá incluir facilidades y herramientas para el monitoreo y gestión de las métricas de acuerdos de nivel de servicios tanto en la estructura operacional de servicios interna como en la interacción y control de los proveedores.

La solución deberá integrarse con las herramientas de monitoreo y gestión de eventos, permitiendo acciones de resolución de fallas de la infraestructura monitoreada basada en umbrales establecidos.

Deberá incluir la gestión de la programación del ciclo de revisión y renovación de SLA's, OLA's y contratos de proveedores.

Se deberá incluir las siguientes funcionalidades:

- Control de contratos de acuerdos de servicio, notificando de forma automática la superación de umbrales especificados antes del incumplimiento del acuerdo.

- Facilidades para la presentación de informes contra los requerimientos de SLA. Por ejemplo, los informes de logros de servicios contra SLA, informes de las razones de infracciones de los SLA informes de excepciones contra los SLA.
- Posibilidad de notificar de forma individual y grupal los eventos que se presenten.
- Facilidades para registrar casos y eventos abiertos y las actividades relacionadas como apoyo al personal de los grupos de soporte.

La herramienta deberá ser personalizada en base a las necesidades funcionales de cada usuario.

3.9. REPORTES

Se deberá generación de reportes estadísticos (Mínimo: soportes pendientes, cantidad de soportes atendidos por cada agente, tipo de evento, frecuencia de un evento, eventos cerrados.)

Los reportes deben ser fácilmente configurables, parametrizables y deben incluir facilidades de generar archivos exportables en formatos como Excel y PDF.

La solución diseñada deberá incluir herramientas para generación de tableros de control con la información de Indicadores Clave de Gestión (KPIs), mostrando un panel de control con opciones gráficas que resuman la información más relevante para análisis gerencial y de control de resultados de gestión, incluyendo facilidades de profundización de la Información y navegación hacia la información de detalle en un esquema de reportes dinámicos.

3.10. GESTIÓN DE ACTIVOS.

La solución diseñada deberá permitir realizar el siguiente inventario de los activos de TI.

- Hardware incluido en cada estación de trabajo (Ej. Procesador, capacidad de disco duro, capacidad de RAM).
- Software instalado teniendo en cuenta: sistema operativo, versiones y licencias.
- Datos financieros del inventario registrado.

Deberá poseer un perfil de administrador que pueda realizar las siguientes opciones del sistema:

- Actualización automática de los cambios registrados en el inventario de hardware o software.
- Gestión del ciclo de vida de los activos (cualificación y cuantificación del uso del activo: estado, historial, tiempo de vida, métricas).
- Estado de equipos: activo, inactivo, dañado, obsoleto, dado de baja.
- Gestión de mantenimientos de activos.
- Gestión de licencias instaladas vigentes y no vigentes.
- Software instalado y no autorizado.

3.10.1. MEDICIÓN DE TRÁFICO.

El diseño deberá permitir la gestión y medición del tráfico de la red de telecomunicaciones asociada al servicio de conectividad ofrecido.

Se monitoreará todos los servicios de conectividad, principalmente los siguientes:

- Tiempo de actividad (*"uptime/downtime"*).
- Ancho de banda.

Se deberá establecer mecanismos de alarmas cuando se sobrepasen los umbrales definidos (Ej. Tiempo de inactividad)

Se deberá establecer mecanismos de alertas de los estados de las métricas monitoreadas (notificación, advertencia, falla)

Permitirá clasificar el tráfico de red (tráfico de entrada y de salida).

Se generará información y reportes gráficos en tiempo real e histórico del servicio de conectividad, manejando un control de autenticación y seguridad de acceso.

3.11. CONTROL REMOTO

El diseño permitirá tomar el control remoto completo de las estaciones de trabajo desde la consola de administración, permitiendo al operador de soporte remoto realizar "*logon, logoff*" o reinicio del equipo a través de la sesión remota, manejar niveles de seguridad de acceso, permitir el control de los equipos a través de una interfaz Web y manejar un control de autenticación y seguridad de acceso.

CAPÍTULO IV:

DESARROLLO DEL SISTEMA.

4.1 SOLUCIONES TECNOLÓGICAS

4.1. ANÁLISIS DE ARQUITECTURA

Definir la arquitectura tecnológica necesaria en el proyecto

4.1.1. ANÁLISIS

Para definir una arquitectura tecnológica para el proyecto, es fundamental identificar las necesidades o requerimientos que dan origen al planteamiento del mismo.

Una vez establecidos los requerimientos, el siguiente paso es enfocarnos en la arquitectura tecnológica a ser utilizada para atender una necesidad y garantizar que se cumpla con el objetivo del proyecto.

4.1.2. REQUERIMIENTOS

Los requerimientos inicialmente establecidos se basan en la definición del proyecto, la misma que ha sido fundamentada según los lineamientos estratégicos de la Dirección de Acceso Universal del MINTEL.

Dentro del marco de los programas y proyectos desarrollados por el MINTEL se ha dotado de equipamiento y conectividad a Infocentros a nivel nacional. Actualmente se cuenta con 491 Infocentros implementados y se encuentra en proceso de implementación un total de 291 Infocentros adicionales. Es decir se tiene 781 sitios que requieren un control y monitoreo para lo cual se contempla el presente estudio.

Se resumen a continuación los requerimientos definidos:

- Contar con un sistema integral que permita realizar la administración, monitoreo y generación de reportes de la infraestructura tecnológica implementada por el MINTEL en los Infocentros.
- Contar con una herramienta que permita garantizar el uso eficiente de los recursos entregados por el MINTEL.

En función de plantear una solución integral enfocada en los beneficiarios directos que hacen uso de la infraestructura y servicios tecnológicos, las necesidades específicas del proyecto se traducen de la siguiente manera:

- Implementar una herramienta para el monitoreo de los enlaces de red.
- Monitorear el funcionamiento del equipamiento informático.
- Administración remota de los equipos a través de una interfaz web.
- Notificación sobre fallos a través de correo electrónico u otros medios.
- Monitoreo de toda la red desde una sola consola de gestión.
- Implementar una herramienta para el manejo y control de contenidos de navegación en internet.
- Contar con una mesa de servicios para el soporte y mantenimiento de los sistemas a ser implementados con niveles de escalamiento y asignación de eventos hacia el MINTEL.
- Contar con una herramienta para la distribución de contenidos digitales desde una consola central de administración, hacia las estaciones de trabajo de los diferentes beneficiarios.

4.1.3. NECESIDADES

En base a la definición de los requerimientos, se plantea las necesidades que deben ser atendidas y garantizadas para posteriormente definir la arquitectura tecnológica que soporte los servicios a proveerse.

En la siguiente tabla se describen los servicios definidos para el proyecto:

N°	Servicio
1	Monitoreo de conectividad de los enlaces de red
2	Monitoreo de equipamiento informático
3	Mesa de servicios y soporte
4	Administración, control y distribución de contenidos.
5	Generación de reportes e indicadores de desempeño.

4.1.4. DISEÑO DE LA ARQUITECTURA

La arquitectura tecnológica debe contemplar los elementos necesarios para soportar y garantizar la gestión y administración de la infraestructura y servicios tecnológicos, deben ofrecer:

- Monitoreo de red y equipamiento informático
- Control de acceso y navegación
- Distribución de contenidos
- Generación de reportes

4.1.5. COMPONENTES DE MONITOREO DE RED Y EQUIPAMIENTO INFORMÁTICO

Actualmente no existe un centro de monitoreo y soporte para controlar y administrar la infraestructura tecnológica entregada por el MINTEL.

Para realizar el monitoreo en primera instancia es necesario la utilización de protocolos y servicios estándares de red como: DNS, DHCP, SMTP, HTTP, HTTPS, IMAP, POP3, FTP, entre otros, mediante la instalación de un agente que envíe el estado de los enlaces y los equipos a un sitio central. Para lo cual en necesario:

- Hardware
    - Servidores físicos o virtuales
    - Storage
    - Switch y router
- Software
    - Sistemas operativo base
    - Software de monitoreo
    - Sistema de virtualización
- Recursos adicionales
    - Configuración de los equipos de red
    - Racks
    - Climatización
    - Sistemas de seguridad
    - Equipo de trabajo con mobiliario

4.1.6. COMPONENTES PARA EL CONTROL DE ACCESO Y NAVEGACIÓN

Considerando la integración de sitios a través de internet, el control de navegación de contenidos puede ser realizado mediante la gestión de políticas desde un sitio central, mediante el monitoreo del tráfico de salida, así para cada petición de salida a internet realizada desde una computadora específica, se monitorea la petición de salida a internet.

Lo cual implica componentes de hardware y software y configuraciones de los equipos de ruteo de los operadores de servicio.

4.1.7. COMPONENTES PARA DISTRIBUCIÓN DE CONTENIDOS

Una alternativa adecuada para la distribución de contenidos, considerando una integración de sitios a través de internet implica:

- Hardware
  - Servidores físicos o virtuales para DNS, monitoreo y contenidos.
  - Storage
  - Switch
  - Firewall
- Software
  - Sistema operativo base
  - Sistema de virtualización
  - Sistema de monitoreo
  - Sistema de distribución de contenidos

4.1.8. ALTERNATIVAS DE IMPLEMENTACIÓN DE COMPONENTES

La administración y gestión de la información puede realizarse considerando una de las siguientes alternativas:

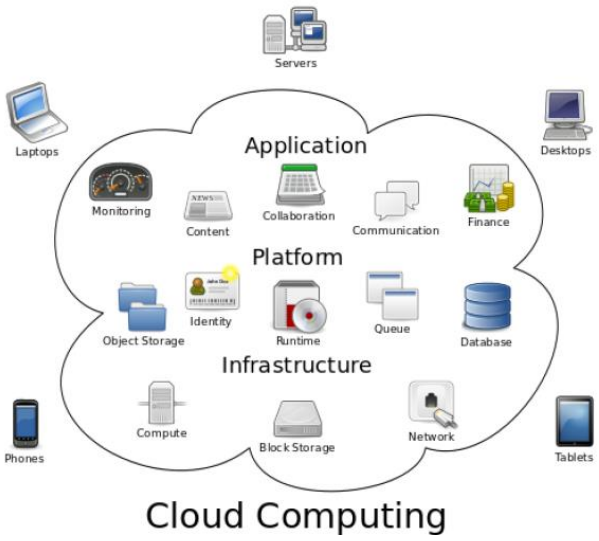
- Contratando servicios de una plataforma para administración y gestión en la nube.
- Implementando infraestructura propia para equipar un Centro de Operación de Red (NOC)
- Realizando un esquema híbrido que incluya servicios en la nube e infraestructura propia.

4.1.9. SERVICIOS EN LA NUBE

Los servicios en la nube proporcionan software, procesamiento y acceso a datos sin que la institución tuviera que implementar hardware, software o contenido en sus instalaciones locales.

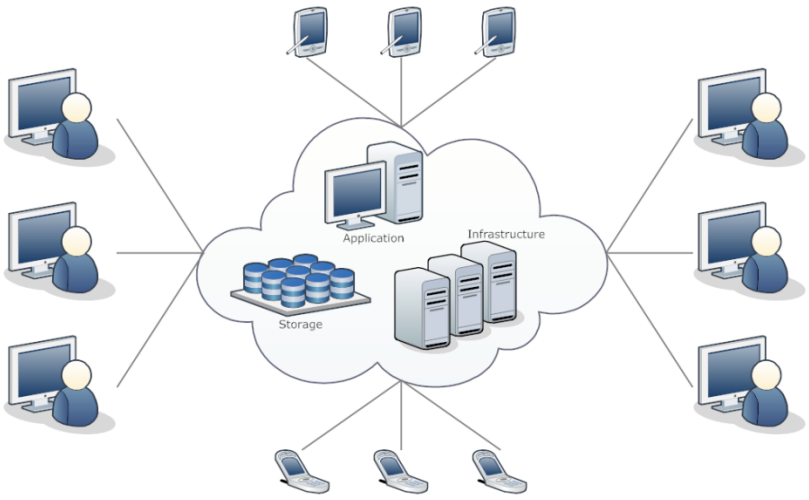
Los servicios en la nube se dividen en tres categorías:

- Infraestructura como servicio (IaaS)
- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)



Para el usuario final de servicios en la nube es transparente el lugar donde se encuentre la infraestructura involucrada para el funcionamiento de las aplicaciones de uso diario que pueden ser utilizadas desde sus dispositivos comunes.

A continuación se presenta un esquema representativo de un servicio de IT en la nube, en el que los diferentes dispositivos tecnológicos se encuentran conectados a Internet para su funcionamiento.



Mantener los datos en un servicio en la nube involucra un ahorro de recursos operativos y administrativos en comparación con la instalación de infraestructura propia, pero se debe considerar un riesgo en cuanto a la confidencialidad y protección de la información, así como la garantía de que el servicio este cien por ciento disponible.

Infraestructura como servicio (IaaS)

Por sus siglas en inglés Infrastructure as a Service (IaaS), se basa en la virtualización para la provisión de recursos computacionales de procesamiento, almacenamiento y red. Ofrece bajo demanda, servicios que permiten remplazar la necesidad de adquirir equipos físicos a los clientes, lo cual incluye el centro de datos donde se alojan los equipos.

Plataforma como servicio (PaaS)

Por sus siglas en inglés Platform as a Service (PaaS) se basa en la entrega de una plataforma ya instalada, configurada y lista para que el usuario final pueda desarrollar y poner en funcionamiento aplicaciones.

Software como servicio (SaaS)

Por sus siglas en ingles Software as a Service (SaaS) se basa en ofrecer a los clientes aplicaciones totalmente funcionales para su inmediata utilización, esto incluye la infraestructura tecnológica, sistemas operativos, configuraciones, mantenimientos y programación necesarios para su funcionamiento.

Estas soluciones tiene la característica de ejecutarse en diferentes dispositivos y encontrarse disponibles para los usuarios a través de una conexión a internet. Dependiendo de la empresa que provea el servicio, las aplicaciones pueden o no tener parámetros configurables de acuerdo las necesidades del usuario..

4.1.10. IMPLEMENTACIÓN DE INFRAESTRUCTURA PROPIA

La consideración de implementación de infraestructura propia involucra la adquisición de hardware, software, procesamiento, acceso y gestión de los datos desde las instalaciones locales del MINTEL.

El hardware, que involucra todos los elementos que deben interactuar para el correcto funcionamiento del sistema, debe ser instalado en un espacio físico adecuado que garantice condiciones de seguridad y climatización, así mismo el software para la gestión de red debe ser instalado en un servidor físico o virtual para su funcionamiento.

El esquema que se implementaría deberá ser centralizado, constituido por un único centro de operaciones ubicado en la ciudad de Quito en las instalaciones del MINTEL.

4.1.11. IMPLEMENTACIÓN HÍBRIDA

Este tipo de implementación implica una convergencia de las soluciones mencionadas anteriormente, en donde unos servicios pueden ser implementados en la nube y otros mediante infraestructura propia.

4.1.12. COMPARATIVA DE ALTERNATIVAS DE IMPLEMENTACIÓN

Se presenta a continuación una matriz comparativa de los criterios más relevantes en la implementación de servicios en la nube y de infraestructura local para la gestión y administración de información.

Característica	Cloud Computing	Infraestructura Propia
Objeto	Modelo de implementación de un servicio mediante una plataforma de virtualización.	Modelo en el que se instala y administra toda la infraestructura tecnológica dentro de la organización.
Se compra	Un servicio.	Equipamiento tecnológico.

Ahorro	Tiempo, esfuerzo y costos de operación.	Una sola compra, se tiene que incluir costos de mantenimiento.
Operación	Se puede obtener un servicio especializado.	Es necesario contratar personal con el conocimiento necesario para la operación y administración.
Enfoque de esfuerzos	Permite externalizar actividades no estratégicas.	Se debe centrar esfuerzos en actividades que no son claves.
Recursos	Se contrata solo lo que se necesita.	Se debe dimensionar toda la infraestructura requerida, sujeto a la obsolescencia.
Escalabilidad	Flexibilidad para aumentar recursos, sujeto a costos.	Poca flexibilidad, cambios grandes implica costos altos.
Seguridad	Percepción de inseguridad, se deben establecer acuerdos de confidencialidad.	Control total de la información, sujeto a políticas propias de seguridad.
Dependencia	La disponibilidad depende del proveedor y de la conectividad.	La disponibilidad depende del administrador.

4.2. ANÁLISIS GENERAL DE ALTERNATIVAS

Se realizó un análisis de varias alternativas nacionales y extranjeras, de soluciones tanto en hardware y software entre las que podemos considerar las siguientes:

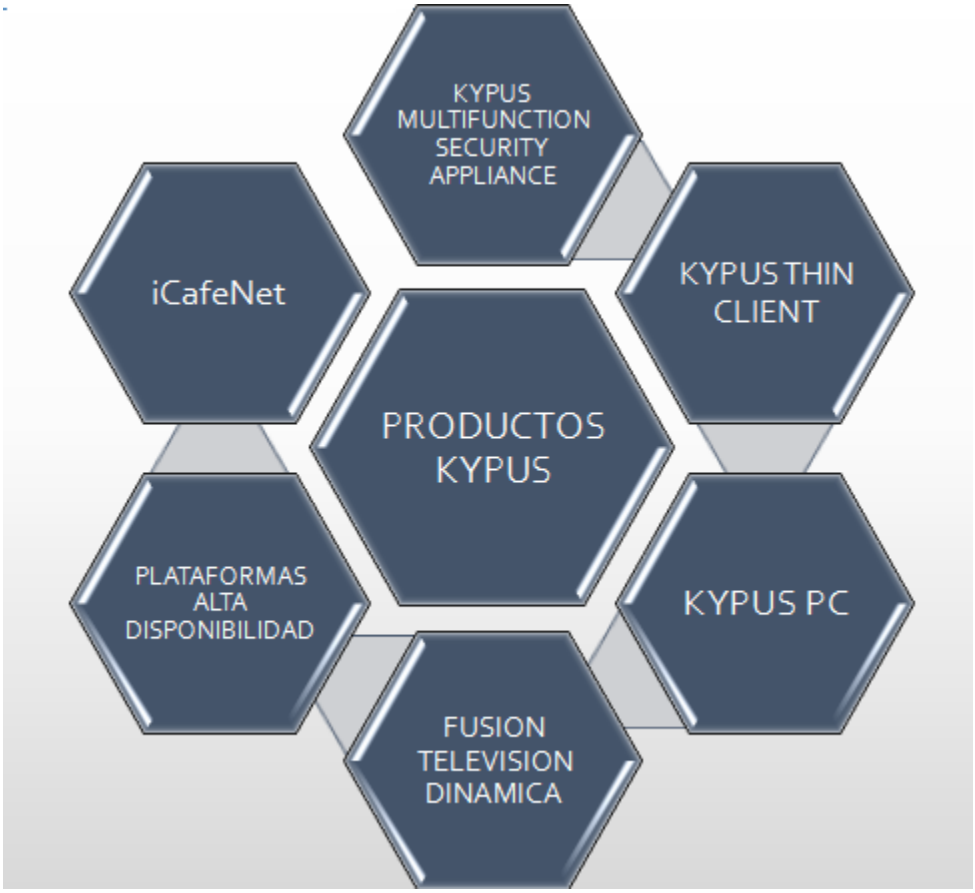
- Icafenet Kypus Nova Device Solución Nacional
- TESEO Vital Innova
- Ártica Soluciones Tecnológicas
- entre otros.

4.2.1. ALTERNATIVA NACIONAL.

4.2.1.1. ICAFENET KYPUS NOVA DEVICE

Nova Devices S.A., es una compañía, de capitales económicos e intelectuales totalmente ecuatorianos, que desarrolla tecnología de punta en la Industria de la Tecnología de la Información, altamente comprometida con la investigación y desarrollo continúo de productos y servicios de Internet e Intranet.

4.2.1.1.1. PRODUCTOS OFERTADOS.



4.2.1.1.2. SOLUCIÓN APLICADA A NUESTRO DISEÑO

La solución aplicada para nuestro diseño se basaría en al iCafeNet, el mismo que es un sistema modular que agrupa los principales componentes que una red necesita para su correcto uso, monitoreo y gestión a lo largo del tiempo. Es compatible con prácticamente

todas las tecnologías presentes, garantizando así su vigencia y valor en el largo plazo. Mide y controla los estándares de servicios pre establecido (SLA).

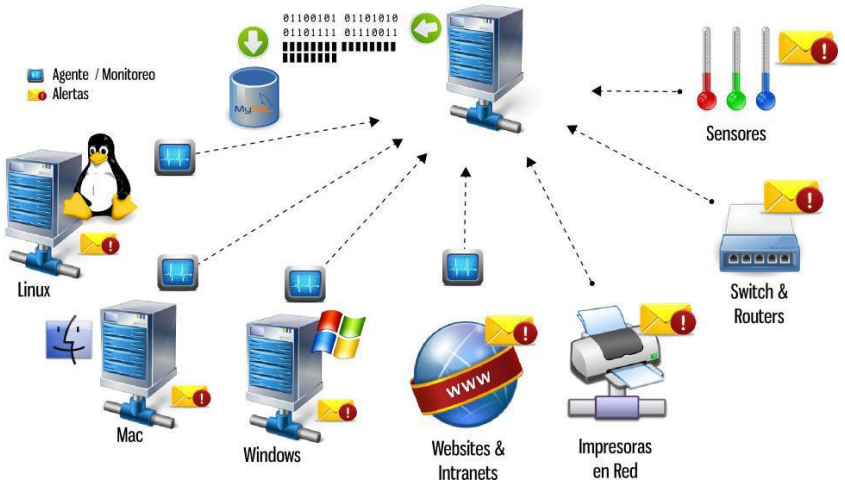
Los módulos actuales del iCafe.Net permiten, además del control y monitoreo de la red, la explotación de servicios directos e indirectos, sean estos de pago público o no, lo cual se traduce en una herramienta para la sostenibilidad de una red orientada al servicio de los usuarios.

4.2.1.1.3. MÓDULOS

- MONITORIZACIÓN
- INVENTARIOS DE SOFTWARE Y HARDWARE
- HELPDESK
- PUBLICIDAD
- TARIFACIÓN Y FACTURACIÓN (servicios directos e indirectos)
- REPORTES DE USO DE INFOCENTROS
- SISTEMA DE ACTUALIZACIONES AUTOMÁTICAS
- SISTEMA DE DISTRIBUCIÓN Y ENTREGA DE CONTENIDOS
- PLATAFORMA DE APRENDIZAJE INTERACTIVO (e-Learning)

4.2.1.1.4. MONITORIZACIÓN

Es una solución de monitorización de red integrada, que ofrece una multiplicidad de características en un solo paquete:



Alta Disponibilidad y rendimiento. El sistema está contemplado para trabajar con un millón de dispositivos en red o más, puede crecer en forma escalable según necesidad del cliente. Trabaja en forma redundante y garantiza la disponibilidad y almacenamiento de datos.

Soporte para SNMP, IPMI, JMX, monitoreo VMware, recopilación de datos deseados a intervalos personalizados, la recolección de la información se la puede realizar mediante servidor/proxy y por agentes.

Definiciones de umbrales flexibles, se pueden definir umbrales de problemas muy flexibles, llamados desencadenantes, haciendo referencia a los valores de la base de datos back-end.

Alerta Altamente configurable, el envío de notificaciones se pueden personalizar, destinatario, tipo de notificaciones, se pueden hacer acciones automáticas, que incluyen comandos remotos.

Gráfica en tiempo real, los elementos monitorizados son inmediatamente graficados utilizando la funcionalidad integrada de gráficos:

Capacidades de monitoreo Web, la herramienta puede seguir un camino de clics del ratón simulados en un sitio web y comprobar la funcionalidad y el tiempo de respuesta.

Amplias opciones de visualización, capacidad de crear gráficos personalizados que pueden combinar varios elementos en una sola vista de mapas de la red pantallas personalizadas y presentaciones de diapositivas para una visión de estilo tablero, informes de alto nivel, vista de recursos supervisados.

Almacenamiento de datos histórico, los datos almacenados en una base de datos de historia configurable incorporado en el procedimiento, incluso con sistema de limpieza.

Fácil configuración, añadir dispositivos supervisados como anfitriones que son recogidos para el seguimiento, una vez en la base de datos aplicar plantillas para dispositivos supervisados es extremamente fácil.

Permite agrupar controles en las plantillas, plantillas pueden heredar otras plantillas

Detección de redes, descubrimiento automático de dispositivos de red mediante el registro automático del agente, descubrimiento de sistemas de archivos, interfaces de red y OIDSNMP Interfaz web veloz, una interfaz basada en la web en PHP accesible desde cualquier lugar.

API que proporciona una interfaz programable para manipulaciones masivas, para integración de software de terceros y otros fines.

Sistema de permisos, autenticación de usuario segura. Algunos usuarios pueden limitarse a ciertos accesos a la herramienta.

El monitoreo se puede implementar tanto en Linux y Windows.

Permite el monitoreo de máquinas virtuales.

4.2.1.1.5. FUNCIONAMIENTO

El software recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente ("agente de inventario"). Puede utilizarse para visualizar el inventario a través de una interfaz web. Tiene la posibilidad de implementación de aplicaciones en los equipos de acuerdo a criterios de búsqueda. Además, existen otras opciones más como escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente.

4.2.1.1.6. COMPONENTES:

El servidor de administración utiliza Apache, MySQL y Perl. Es multiplataforma y gracias a su simple diseño, el rendimiento del lado del servidor es muy bueno. Un servidor con relativamente pocos recursos podría realizar el inventario de miles de máquinas sin ningún tipo de problemas. El servidor, puede ser instalado en los siguientes sistemas operativos:

- GNU/Linux (Ubuntu, Debian, Suse, RedHat, Gentoo, Knoppix, Slackware, Mandriva, Fedora y Centos), FreeBSD,
- Windows (XP, 2000, server 2008. 2012R2),
- Sun Solaris.

4.2.1.1.7. AGENTES

- Para recoger el máximo de la información posible, hay agentes que pueden ser instalados en los equipos clientes. Estos agentes están disponibles para:
- GNU/Linux (Ubuntu, Debian, Suse, RedHat, Gentoo, Knoppix, Slackware, Mandriva, Fedora y Centos),
- Windows (95, 98, NT4, 2000, XP, server 2003, Vista, 7,8),

- Mac OS X,
- Sun Solaris.

4.2.1.1.8. DESVENTAJAS.

La principal desventaja es que, al tratarse de solución nacional y al ser el proyecto infocentros un “Proyecto Emblemático Cinco Estrellas”, con un gran impacto social económico y político del cual no se han desarrollado proyectos similares l en el país, la solución nacional no cuenta con la experiencia necesaria para oferta este tipo de proyectos, por lo que se descarta la utilización de este solución.

4.2.2. ALTERNATIVA INTERNACIONAL.

4.2.2.1. TESEO VITAL INNOVA

TESEO, es una aplicación desarrollada por la empresa Vital Innova para la Universidad de Extremadurade España para la gestión y monitores de los telecentros implementados por Diputaciones y Ayuntamientos de España, estos telecentros utilización un sistema operativo basado en LINUX.

4.2.2.1.1. CARACTERÍSTICAS DEL SOFTWARE

Teseo ofrece servicios tanto para los facilitadores de los infocentros (denominados Dinamizadores por Vital Innova), como para todos aquellos perfiles que participan en la coordinación y administración de una red de infocentros.

Los servicios más importantes incluidos en Teseo para el perfil Facilitador son los siguientes:

- Visualización del estado de los equipos de la sala en tiempo real.
- Encendido, apagado y reiniciado remoto de equipos de usuario.

- Escritorio remoto y envío de mensajes a los puestos de usuario.
- Control de tiempo de sesión en equipos de usuario.
- Gestión de cuentas de acceso.
- Registro automático de sesiones de usuario.
- Reserva de equipos para capacitaciones programadas.
- Gestión de actividades formativas.
- Cuadro de mando local. Informes y estadísticas.
- Gestión económica (Módulo de control de costos e ingresos).
- Listas de espera de usuarios para cursos y capacitaciones.
- Registro y control de incidencias.

Teseo está compuesto por dos aplicaciones:

4.2.2.1.2. TESEO DINAMIZADOR:

La aplicación Teseo Dinamizador ofrece, además de las funcionalidades necesarias para gestionar una sala parte de un dinamizador, un conjunto de servicios destinados a coordinadores de la red de centros:

- Planificación de actividades formativas y coordinación de formadores
- Cuadro de Mando
    - Usuarios
    - Sesiones
    - Formación
    - Lista de espera
    - Evaluación
    - Auditoría

- Indicadores

- Gestión de Actividades
- Presupuestos
- Plan Formativo
- Gestión de Convenios

4.2.2.1.3. PLANIFICACIÓN DE ACTIVIDADES FORMATIVAS.

El módulo de planificación de actividades permite, a un coordinador, ver la planificación de actividad los centros en función de un conjunto de parámetros de consulta. Por otra parte, le permite validar la información de la planificación de actividad, y establecer la planificación de actividades en el calendario. Este módulo facilita la coordinación de actividades formativas, así como los formadores o las entidades colaboradoras.

4.2.2.1.4. TESEO USUARIO:

Control de equipos de usuario

Adicionalmente TESEO permite la gestión de la red a un Coordinador General y Coordinadores Regionales con las siguientes facilidades:

- Planificación de actividades formativas y coordinación de formadores
- Cuadro de Mando
- Usuarios
- Sesiones
- Formación
- Lista de espera
- Evaluación
- Auditoría

- Indicadores
- Gestión de Actividades
- Presupuestos
- Plan Formativo
- Gestión de Convenios locales

4.2.2.1.5. DESVENTAJAS.

La principal desventaja al analizar esta alternativa es que al tratarse de un solución gratuita desarrollada para la Universidad Extremadura está basada en la plataforma LINUX por lo que requiere de herramientas adicionales para cumplir su función en sistema operativo Windows dado que proyecto infocentros cuenta con tres componentes con diferentes características técnicas para su implementación (373 implementados a través del convenio PAUTIC que poseen un sistema operativo LINUX, 100 implementados a través del convenio Ecuador Estratégico poseen sistema operativo doble boot LINUX Y WINDOWS y 291 implementados a través de Ampliación de la Red Infocentros poseen un arquitectura cliente servidos con sistema operativo doble boot LINUX Y WINDOWS adicionalmente se cuenta con 17 donaciones que manejas distintos sistemas operativos entre LINUX Y WINDOWS), por tal motivo se requiere que la solución adoptada trabaje con los dos sistemas operativos WINDOWS y LINUX, por este motivo se descarta la aplicación de esta solución.

4.2.3. ÁRTICA SOLUCIONES TECNOLÓGICAS

Solución basada en *Ártica Soluciones Tecnológicas* (http://Ártica.es/) es una solución creada por una compañía privada española de desarrollo de software, con tres productos principales:

- Pandora FMS Enterprise,
- Babel Enterprise e
- Integria.

Con miles de usuarios en todo el mundo.

Pandora FMS, es actualmente una de las soluciones de monitoreo más reconocida en el ámbito nacional e internacional por su excelente relación precio/prestaciones, y por ser una herramienta extremadamente confiable, fácil de aprender y usar, y adaptable a la medida de las necesidades de cada cliente.

Ártica cuenta con una amplia red de "*partners*" en varios países, y tiene una política de fuerte compromiso con cada uno de estos socios tecnológicos, de cara a ofrecer un excelente nivel de servicio de soporte a cada cliente.

Pandora FMS Enterprise cuenta con varias instalaciones funcionando en varias partes del mundo incluyendo América Latina.

4.2.3.1. DIAGRAMA GENERAL DEL REQUERIMIENTO TÉCNICO

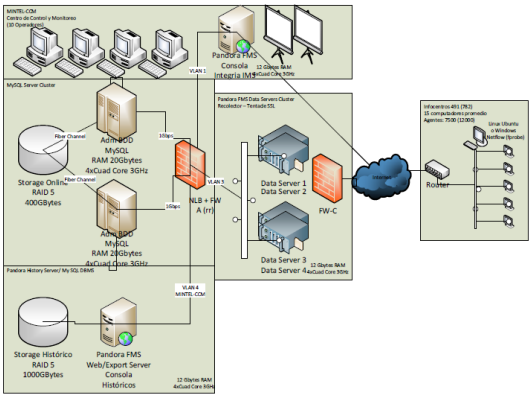


Ilustración 1Topología General del Sistema de Gestión relacionado con la topología existente en los infocentros.

Pandora FMS es actualmente una de las soluciones de monitoreo más reconocida en el ámbito internacional por su excelente relación precio/prestaciones, y por ser una herramienta extremadamente confiable, fácil de aprender y usar, y adaptable a la medida de las necesidades de cada cliente.

Ártica ha trabajado junto con Telefónica de España en su proyecto para monitorear otros 10000 dispositivos. Pandora FMS Enterprise ha reemplazado a herramientas ya implantadas, como HP OVO, HP *"Sitescope"*, HP NNM, Infovista y Cisco Netflow.

4.2.3.2. DESCRIPCIÓN DE LA SOLUCIÓN.

Pandora FMS (Flexible MonitoringSystem) Enterprise es una aplicación de monitoreo capaz de vigilar todo tipo de sistemas y aplicaciones, permitiendo conocer el estado de cualquier elemento de todos los sistemas y procesos de negocio del sistema (hardware, software y aplicaciones), pensada para facilitarles el trabajo a los administradores de sistemas, pero es posible adaptarla a cualquier entorno.

Es un sistema abierto, modular y multiplataforma, que le permite adaptarse a la medida de las necesidades de cada organización, en nuestro caso la Red nacional de Infocentros.

Un diferenciador clave con respecto a otras alternativas del mercado, es que la solución de monitoreo llega al nivel del dato. A diferencia de la mayoría de soluciones que basan su monitoreo solamente en eventos. La solución, además de trabajar sobre eventos, monitorea elementos de datos, lo cual le permite un nivel de monitoreo, gestión y automatización de sistemas, procesos importante para el MINTEL, y que otros no pueden brindarle, esta solución ha sido desarrollada en C++ y Perl, HTML5 y AJAX.

La solución tiene una estructura modular basada en sub-servidores, para cada tipo de chequeo que realiza, su performance es consistentemente y soporta operación en alta disponibilidad, tanto para los servidores recolectores de datos, así como también para los otros servidores de *"Networking"*, WMI, etc. Adicionalmente es posible configurar la Base de Datos MySQL en un ambiente de Data Center con balanceo de cargas por medio de hardware específico designado para el efecto (NBL) o por medio de las herramientas de clúster de Linux o de MySQL.

La solución es una herramienta de monitoreo que no sólo mide si un parámetro está bien o mal, puede cuantificar el estado (bien, mal y valores intermedios) o almacenar un valor (numérico o alfanumérico) durante meses si es necesario, permite medir rendimientos, comparar valores entre diferentes sistemas y establecer alertas sobre umbrales. El sistema trabajará sobre dos bases de datos (una de producción y otra histórica), de forma que puede generar informes, estadísticas, niveles de cumplimiento de servicio (SLA) y medir cualquier cosa que proporcione o devuelva un dato, sobre cualquier período de tiempo que el cliente necesite, es decir, se puede medir casi cualquier cosa; sistemas operativos, servidores, aplicaciones y sistemas hardware, entre lo que podemos mencionar a cortafuegos (firewalls), proxies, bases de datos, servidores web, VPN, routers, switches, procesos, servicios, acceso remoto a servidores, equipos diversos tales como sistemas de radiocomunicaciones, de telefonía IP, cámaras de vigilancia, terminales de punto de venta, etc.

Pandora FMS Enterprise se puede implementar sobre cualquier sistema operativo, con agentes específicos para cada plataforma, por ejemplo en Windows (2000, XP, 2003, 2008, Vista, 7, 8 y 8.1), Linux, Mac, Solaris, HP-UX, BSD, AIX, IPSO, y OpenWRT.

Pandora FMS Enterprise se puede implementar sobre cualquier sistema operativo, con agentes específicos para cada plataforma, por ejemplo en Windows (2000, XP, 2003, 2008, Vista, 7), Linux, Mac, Solaris, HP-UX, BSD, AIX, IPSO, y OpenWRT, esta se compone de 5 capas: recolección, consolidación, visualización, actuación y presentación.

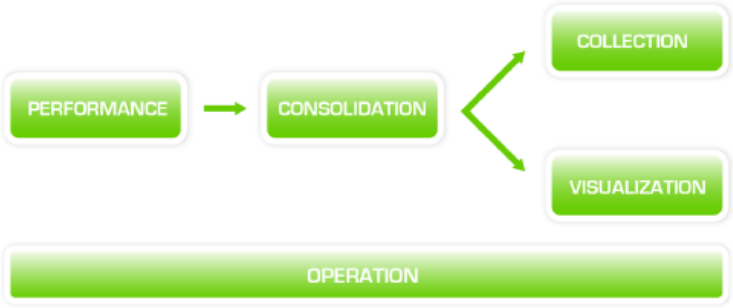


Ilustración 2Descripción General del funcionamiento del sistema

4.2.3.3. CAPA DE RECOLECCIÓN

Esta capa le permite a Pandora FMS Enterprise recolectar información, los componentes que conforman esta capa son los diferentes sub-servidores y los agentes de Pandora FMS Enterprise.

Los servidores de Pandora FMS Enterprise pueden recolectar datos remotamente, o procesar la información enviada por los agentes.

Estos son los diferentes sub-servidores de Pandora FMS Enterprise:

- Data server: procesa todos los datos enviados por los agentes. Puede soportar hasta 3000 agentes por servidor de recolección de datos. Hay que considerar que es posible incrementar en forma lineal el número de servidores, los cuales seguirán recibiendo los mensajes de los módulos de monitoreo y registrándolos en la Base

de Datos, para lo cual se requiere una configuración de la misma orientada a mayor performance.

- Inventory server: recoge datos de inventario remotamente o los enviados por los agentes. Este servidor recoge información sobre hardware, software, aplicaciones, configuraciones, etc.
- Web server: permite monitorear experiencias de navegación de usuario, realizando testeo de autenticación, latencias, estado de los servicios. Soporta múltiples tipos de aplicaciones web, webmail, ecommerce, etc.
- Plugin server: este servidor utiliza scripts para recolectar datos de manera remota. Soporta casi todos los plugins de Nagios.
- Network server: servidor para chequear protocolos de red (ICMP, TCP, SNMP)
- SNMP console: server recibe TRAPS enviados por agentes SNMP.
- WMI server: permite monitorear equipos Windows utilizando el protocolo WMI.
- Recon server: ejecuta tareas de reconocimiento y configura automáticamente los dispositivos descubiertos para ser monitorizados a la vez que genera un mapa de topología de red.
- Export server: exporta datos de una instancia de Pandora FMS Enterprise a otra para poder escalar el despliegue de Pandora FMS.
- Prediction server: brinda la capacidad a Pandora FMS Enterprise de hacer una predicción de futuros comportamientos de los sistemas basándose en el histórico de valores obtenidos.
- SNMP server: servidor de red de alto rendimiento para la realización de consultas SNMP.

- ICMP server: servidor de red de alto rendimiento para la realización de consultas ICMP.

Los agentes de Pandora FMS Enterprise, son livianos, desarrollados en C++ y Perl.

Recolectan los datos localmente y los envían al servidor de Pandora FMS Enterprise para ser procesados. Son sumamente versátiles y dotan a la herramienta de una capacidad de monitoreo prácticamente ilimitada.

Ilustración 3Descripción del funcionamiento de los agentes.

Existen agentes de Pandora FMS Enterprise para Linux, Mac, Solaris, HP-UX, BSD, AIX, IPSO, OpenWRT y Windows (2000, XP, 2003, 2008, Vista, 7, 8 y 8.1).

Los agentes utilizan los módulos para recolectar periódicamente datos. Los módulos son comandos del sistema donde se instala el agente y recolectar información básica de CPU, uso de la memoria, tráfico en los interfaces etc. Para recolectar datos más complejos, los agentes recurren al uso de lo que denominamos plugins.

Los agentes soportan la ejecución de pre o post condiciones, antes o después de ejecutar el módulo para luego ser enviado al servidor de Pandora FMS Enterprise.

Las colecciones de archivos permiten a los agentes descargarse scripts o actualizaciones desde el servidor de Pandora FMS Enterprise.

Los agentes pueden ser configurados para trabajar en alta disponibilidad en activo/activo o activo/pasivo. Si la conexión entre un agente y el servidor, el agente puede almacenar los datos para ser enviados cuando se restablezca la conexión.

La comunicación entre el agente y el servidor se puede realizar utilizado varios protocolos de comunicación:

- SSH: unidireccional, del agente al servidor. Con esta opción no es posible la utilización de la funcionalidad de la configuración remota del agente. Se necesita hacer el intercambio de claves.
- Tentacle: herramienta cliente-servidor que utiliza el puerto TCP 41121. Permite la utilización de la configuración remota del agente así como encriptación SSL.

El agente de Pandora FMS Enterprise permite ser configurado con la opción de proxy, que le permite al agente actuar como proxy para otros agentes, además de monitorear. Esta característica permite la utilización de la configuración remota y las colecciones de archivos.

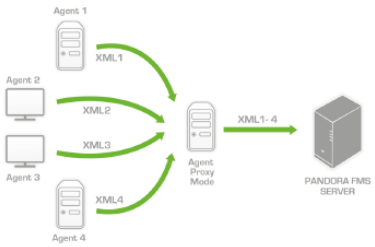


Ilustración 4Descripción del funcionamiento con configurado con la opción de proxy.

El agente también cuenta con un modo broker, que le permite enviar datos como si fueran varios dispositivos. El modo broker es utilizado para la monitoreo de dispositivos remotos que no están accesibles desde Pandora FMS Enterprise.

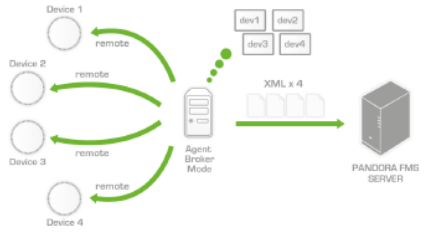


Ilustración 5Descripción del funcionamiento con modo broker

Además del agente software, Pandora FMS Enterprise cuenta con un agente remoto, que no requiere ser instalado en ningún dispositivo. Este agente permite hacer chequeos remotos (TCP, SNMP, WMI, etc) a través de los servidores de Pandora FMS Enterprise.

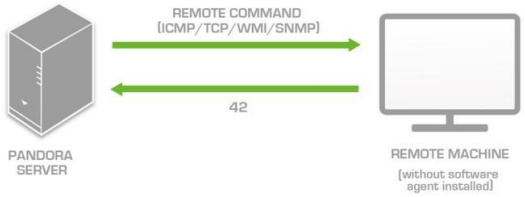


Ilustración 6Descripción del funcionamiento con agente remoto

Es posible combinar ambos tipos de agentes sobre un mismo dispositivo.

Pandora FMS Enterprise cuenta con agentes hardware para medir parámetros ambientales, tales como temperatura, humedad, presencia de líquidos etc.

4.2.3.4. CAPA DE CONSOLIDACIÓN

La solución consolida todos los datos recogidos en una base de datos relacional, existiendo 2 bases de datos.

La base de datos principal es la que almacena los datos más recientes. La base de datos secundaria se utiliza para el almacenaje de datos históricos.

Pandora FMS Enterprise compacta todos los datos para optimizar el espacio utilizado en la base. Esta característica viene configurada por defecto, y puede ser desactivada. Esta opción de compactación permite reducir entre un 40% y un 70% el espacio utilizado.

Todos los datos recogidos pueden ser exportados a la base de datos de históricos, y de esta manera reducir el número de consultas realizadas a la base de datos principal, lo cual redunda en una notable mejora del rendimiento.

Esta característica también mejora el tiempo de respuesta en la creación de informes.

Las bases de datos actualmente soportadas son MySQL, Oracle y PostgreSQL. Se recomienda utilizar la versión Enterprise de MySQL denominada Percona Server.

4.2.3.5. CAPA DE VISUALIZACIÓN

Pandora FMS Enterprise tiene una interface Web multiusuario. Desde la consola se configuran los niveles de accesos para los diferentes usuarios, utilizando para ello un sistema de ACL (Access Control List).

La interface Web se divide en 2 secciones:

La primera sección es la de operación. En esta sección Pandora FMS Enterprise muestra toda la información recogida.

La segunda sección es la de administración, desde la que se realiza la configuración de todos los parámetros.

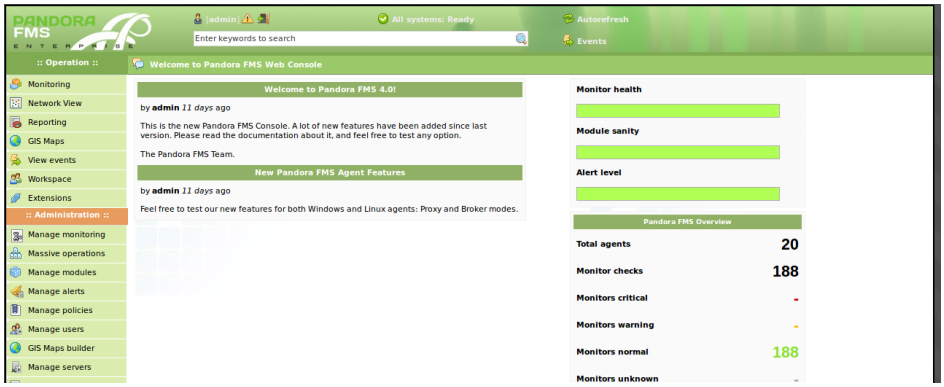


Ilustración 7 Consola de administración

Dentro de la sección de operaciones se puede encontrar toda la información de los diferentes agentes (módulos, alarmas).

Estas son solo algunas posibilidades para la visualización:

4.2.3.6. DASHBOARDS

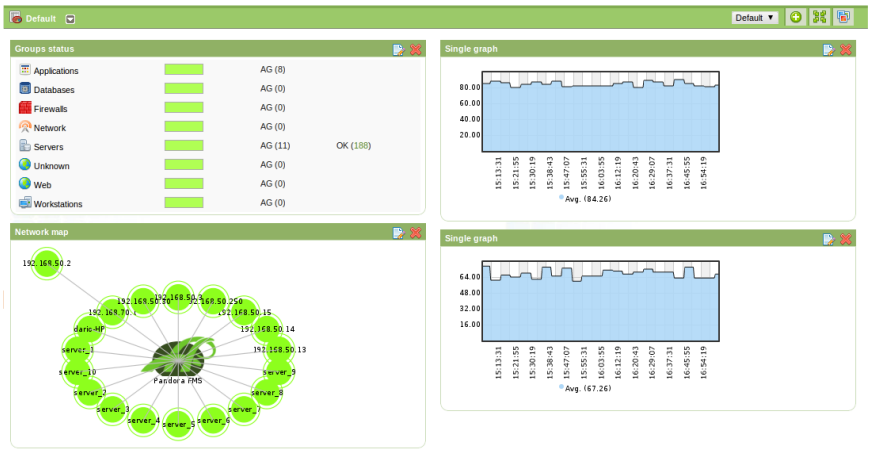


Ilustración 8Consola de administración configuración de parámetros.

Los dashboards o cuadros de mando de Pandora FMS Enterprise son totalmente configurables y están basados en widgets capaces de mostrar diferentes tipos de información, tales como gráficas simples, mapas, métricas, resúmenes de los estados de los grupos configurados, etc.

El MINTEL realizará la creación y configurar su propio dashboard.

4.2.3.7. NETWORK CONSOLE

La Network Console está desarrollada utilizando HTML5, y muestra un mapa con la topología generada por el Recon server. En ella se pueden mover los elementos, añadirlos y eliminarlos.

Cada elemento representa un agente, al dar clic sobre el ícono de un agente, la consola mostrará información detallada del mismo.

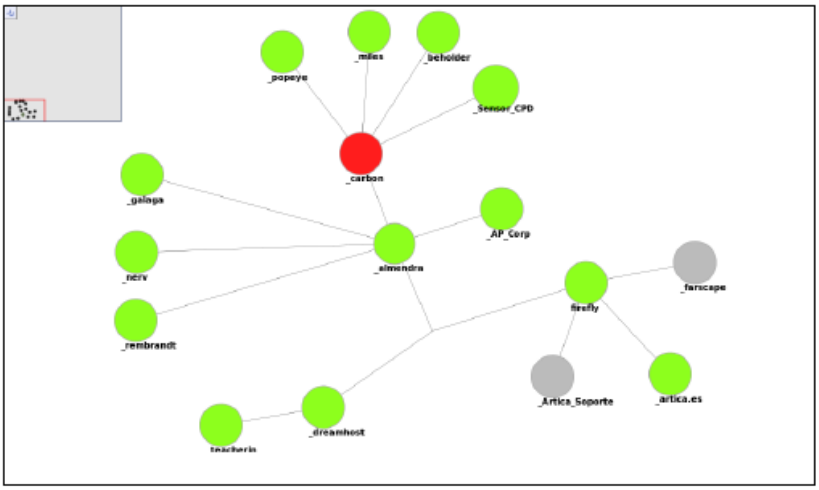


Ilustración 9Consola mapa de topología.

4.2.3.8. VISUAL CONSOLE

Otra forma de visualizar la información es con la Visual Console.

Esta consola permite realizar vistas personalizables.

Se puede crear una vista utilizando el editor de la consola visual, y se pueden añadir múltiples elementos, gráficas, íconos, texto, etc.

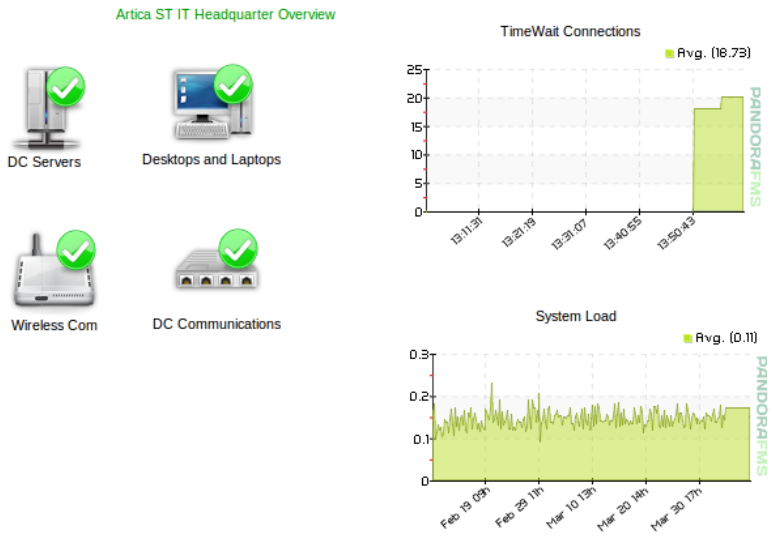


Ilustración 10Consola visualización de estadísticas.

Algunos plugins tales como el de VMWare, tienen su propia consola visual. Esto hace que sea más sencilla la detección de problemas.

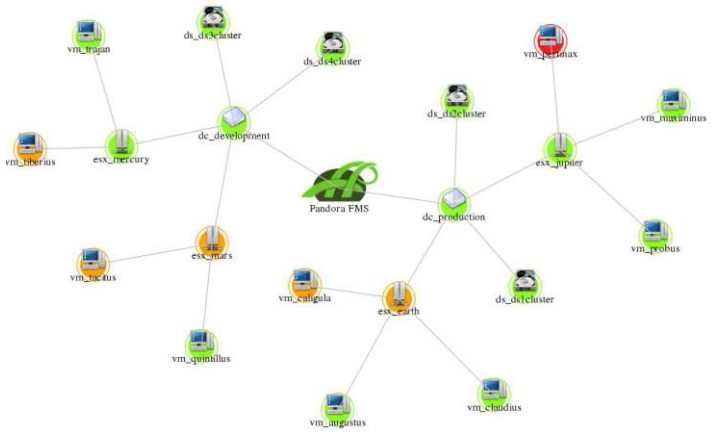


Ilustración 11Mapa de equipamiento

Pandora FMS Enterprise cuenta con una consola de eventos que muestra “qué está pasando”.

La consola de eventos mostrará todos los eventos, como por ejemplo errores, alarmas, o el hecho de que se ha añadido un nuevo agente, incluso se puede configurar los eventos

cuando se produce un cambio en el inventario, de manera que se refleje como un estado crítico o de alerta, lo cual permitirá ver al agente con otro color por efectos de que se incrementó o disminuyó por ejemplo la memoria o el disco de uno de los computadores, o si la CPU que reporta ahora es diferente de la que reportaba en ocasiones anteriores.

Los eventos se pueden filtrar o exportar en formato CSV o RSS.

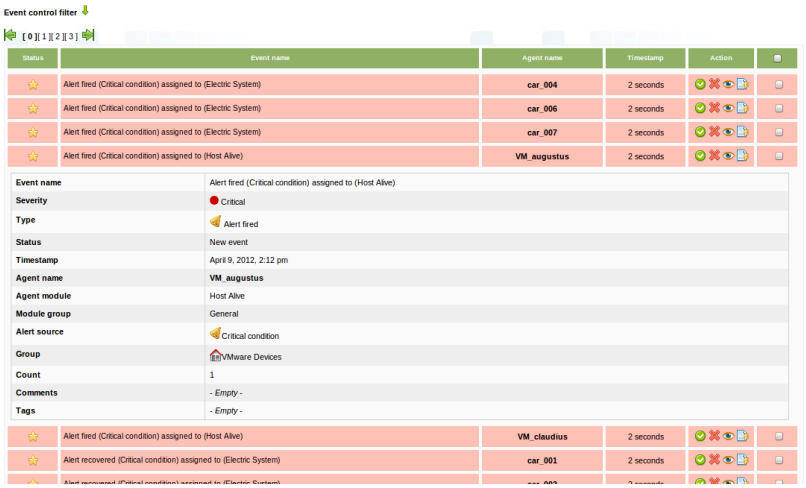


Ilustración 12Consola visualización de eventos.

4.2.3.9. SISTEMA DE REPORTES

Pandora FMS Enterprise tiene un potente sistema de informes, que permite crear informes utilizando información de varios agentes.

La creación de informes es sumamente sencilla gracias a la interface WYSIWYG y a varios elementos predefinidos, tales como: SLA, eventos, métricas ITIL (MTBF, MTTR, TTO y TTRT), gráficas, alertas disparadas mediante umbrales, previsiones y muchos otros elementos más.

Se puede utilizar información de cualquier corte de tiempo (de los últimos 5 minutos⋯ o de los últimos 5 años).

Los informes son 100% adaptables a la medida del usuario, con logos, colores y fuentes, y se pueden generar en HTML, PDF, CSV o XML.

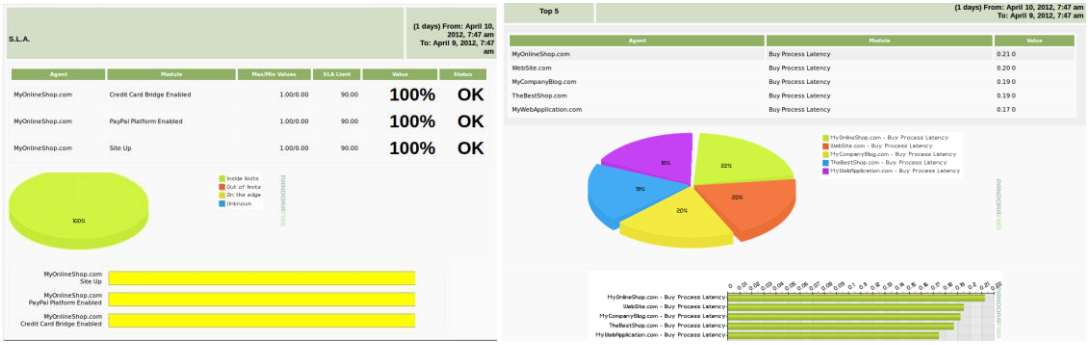


Ilustración 13Consola visualización de informes estadísticos.

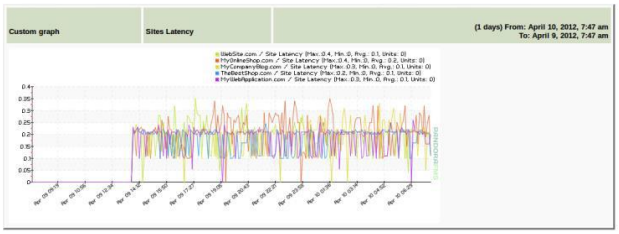


Ilustración 14Consola visualización de informes gráficos.

4.2.3.10. CAPA DE ACTUACIÓN

La capa de actuación reacciona cuando aparece un evento en Pandora FMS Enterprise.

Esta capa ejecuta acciones. Un ejemplo sería cuando un valor supera su umbral configurado, en donde Pandora FMS Enterprise lanzaría una alarma para avisar que algo no es correcto.

Las acciones se pueden configurar para enviar una notificación a través de e-mail, de un SMS, o enviar un TRAPSNMP, o hacer que un agente software ejecute una acción para que reinicie un servicio, entre otras acciones.

Al ser configurable esta capa, es posible añadir más acciones a las que Pandora FMS Enterprise tiene por defecto, utilizando comandos del sistema.

Además de la acción, es posible configurar el comportamiento de la misma (las veces que se ejecuta, cuándo debe ejecutarse, etc). Es posible inclusive poner las acciones fuera de servicio para que no se vean afectadas por la realización de trabajos programados.

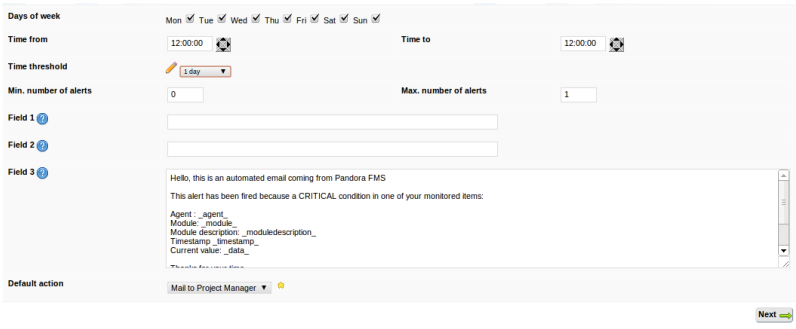


Ilustración 15Consola visualización de informes de acciones fuera de servicio.

Pandora FMS Enterprise puede correlacionar alarmas y generar alertas para informar a niveles superiores como mecanismo de escalamiento.

Pandora FMS Enterprise cuenta con un sistema de protección en cascada, el cual permite evitar una “lluvia” de alertas cuando un grupo de agentes no es accesible por una falla en las comunicaciones.

4.2.3.11. CAPA DE OPERACIÓN

Pandora FMS Enterprise tiene una arquitectura flexible, que facilita su despliegue y su operación. Gracias a su arquitectura basada en múltiples servidores, es posible monitorear miles de dispositivos.

Todos los componentes de Pandora FMS Enterprise soportan alta disponibilidad. También está implementada una solución de duplicación de dispositivos de bloque (DRBD) para

realizar copia de los datos en tiempo real y poder tener replicada la instancia de Pandora FMS Enterprise en diferentes equipos.

Pandora FMS Enterprise cuenta con múltiples características para facilitar su manejo.

4.2.3.12. METACONSOLA

Facilita la gestión de múltiples instancias de Pandora FMS Enterprise desde una única consola. Desde la metaconsola es posible generar informes uniendo todos los datos obtenidos desde las diferentes instancias de Pandora FMS Enterprise.

4.2.3.13. POLÍTICAS

Las políticas sirven para crear plantillas de monitoreo. Con las políticas es posible crear plantillas con módulos, alertas, colecciones e inventarios, y asignárselo a los agentes.

Es una forma de homogeneizar el monitoreo, ya que una configuración de monitoreo válida para un sistema puede ser aplicada a miles de sistemas, en forma sencilla y automatizada.

Las políticas también permiten la creación de grupos lógicos de agentes.

4.2.3.14. CLI (Command Line Interface)

Pandora FMS Enterprise permite realizar por comandos las mismas acciones que desde la consola web, desde la línea de comandos. Es un método especialmente útil para integrar aplicaciones de terceros con Pandora FMS Enterprise.

4.2.3.15. INTEGRIAIMS

Es una herramienta que nos permite hacer la gestión integral para los Infocentros y equipos de trabajo. IMS son las siglas de “ITIL Management System”, lo que implica que Integria sirve para gestionar desde el punto de vista de ITIL.

A un nivel más funcional, podemos definir Integriaims como una herramienta para la gestión de proyectos, recursos humanos, imputación de horas/time tracking, seguimiento de tickets, combinado con un completo sistema de inventario, y un sistema de CRM (gestión de clientes), un Wiki, gestión de asignación de tareas, una Base de conocimiento, un sistema de distribución de ficheros y algunas otras funcionalidades más. Todo ello vía WEB, multiusuario/multiperfil.

Existe una parte Enterprise de Integriaims, que añade un sistema de ACL basado en usuario, grupo y perfil para controlar el acceso a los diferentes elementos de Integriaims. Es lo que diferencia principalmente la versión Open Source de la versión Enteprise.

4.2.3.16. CARACTERÍSTICAS GENERALES.

- Gestión de tickets de mesa de ayuda (ticketing)
- Gestión de proyectos
- Gestión de tiempo (time tracking)
- Gestión de conocimiento (knowledge base)
- Sistema de Inventario (CMDB)
- Agenda
- Wiki
- Gestión de leads, empresas, contratos, contactos y facturas (CRM)
- Entorno centralizado de descargas de software
- Control de personal

4.2.3.17. GEO-LOCALIZACIÓN PARA AGENTES.

Pandora FMS Enterprise puede proporcionar información de localizaciones y mapas interactivos que muestren la posición de los agentes. También puede mostrar el rastro

(tracking) del recorrido de cada agente a lo largo del tiempo, haciendo una geo-localización inversa y "traduciendo" las coordenadas en direcciones "legibles".

4.2.3.18. PRINCIPALES CARACTERÍSTICAS.

Pandora FMS Enterprise es un potente sistema de monitoreo multi-plataforma.

Ártica escucha a sus clientes, y aprende de ellos. En forma permanente.

Las continuas mejoras en Pandora FMS Enterprise se basan en las propias necesidades de sus usuarios.

Pandora FMS Enterprise les brindará a ustedes múltiples beneficios, con una misma solución.

A continuación mencionamos algunos de los beneficios que Pandora FMS Enterprise podría proporcionarles:

- **Escalabilidad virtualmente ilimitada**

  Pandora FMS Enterprise es la misma herramienta, y le sirve por igual a un cliente que necesita monitorear 25 sistemas, como a un cliente que requiere gestionar decenas de miles de sistemas.

  Pandora FMS Enterprise tiene una arquitectura modular y escalable, que brinda al cliente todas sus ventajas sin importar el tamaño de su plataforma, y puede ir escalando conforme el cliente amplíe el alcance del monitoreo, sin que por ello disminuya la performance del sistema.

- **Aplicaciones a medida.**

  Ártica atiende a las necesidades del MINTEL.

Y responde a sus requerimientos con soluciones que incorpora a las prestaciones de Pandora FMS Enterprise.

La evolución y el éxito de Pandora FMS Enterprise están basados en este foco puesto sobre el cliente.

Este es otro beneficio clave que los usuarios de Pandora FMS Enterprise valoran: la flexibilidad del fabricante en adaptar su solución a sus necesidades beneficio que no encuentran en otras alternativas, que por añadidura resultan significativamente más costosas.

- **Garantía de permanente evolución tecnológica**

Pandora FMS Enterprise es una solución en constante evolución.

Y no solamente a través de su permanente actualización en nuevas versiones, como la que Ártica próximamente lanzará con Pandora FMS Enterprise release 5.1 SP2, sino mediante las continuas mejoras y "customizaciones" que tanto Ártica como sus partners realizan a pedido de los clientes.

Podemos afirmar sin temor a equivocarnos que Pandora FMS Enterprise está realmente a la vanguardia tecnológica en materia de monitoreo y gestión automatizada de múltiples entornos físicos y lógicos, y con una relación precio/prestaciones de entre 7 y 10 a 1 con respecto de otras opciones del mercado.

4.3. CUADRO COMPARATIVO DE CARACTERÍSTICAS TÉCNICAS DEL SISTEMA

CONDICIONES GENERAL					
ÍTEM	REQUERIMIENTO	Ártica Soluciones Tecnológicas		TESEO	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
1	Solución integral de un centro de gestión de servicios de TI.	X		X	
2	Versión alineada a los procesos de la Biblioteca de la Infraestructura de las Tecnologías de Información (ITIL), EV: Administración de Eventos, IM: Administración de incidentes, KM: Administración del Conocimiento, SACM Administración de Servicios y Configuraciones, SCM Inventario del Catálogo de Servicios registrado, SLM Información para Control de Cumplimiento de los Niveles de Servicio	X		X	
3	Funcionamiento multiplataforma (mínimo Windows y Linux)	X			X
4	Criterios de flexibilidad, escalabilidad, redundancia, alta disponibilidad, además debe contar con medidas de contingencia que permitan asegurar la continuidad del servicio y la recuperación de desastres.	X		X	
5	Incluir funcionalidades del mismo fabricante que faciliten la gestión de inventarios de hardware y software, control remoto, registrode cambios y configuraciones, registro de eventos, gestión de incidentes, gestión de activos y herramientas de monitoreo tanto pasivo como proactivo de las plataformas.	X		X	
6	Gestión de hardware se requiere llevar un inventario del equipamiento informático con las capacidades de los computadores como: tipo de procesador, velocidad de procesador, capacidad de discos duros, capacidad RAM. En cuanto al software se requiere el inventario del software instalado teniendo en cuenta las versiones y licencias.	X		X	
7	Todo software incluido debe ser instalado y configurado para garantizar la compatibilidad e interoperabilidad del sistema.	X		X	
8	Todo software requerido, deberá ser instalado, configurado y se realizarán las pruebas de verificación de cumplimiento.	X		X	
9	El sistema debe permitir establecer parámetros de configuración de umbrales de operatividad, correlación de eventos y definición de la menos 3 mapas de servicio.	X		X	
10	Implementación del hardware y software necesarios para un centro de monitoreo y de una mesa de servicios con mínimo 10 licencias nombradas para las siguientes funcionalidades: Service Desk (Incidentes y Problemas), Change (Gestión de Cambios), Asset (Gestión de Activos), ServiceLevel (Gestión de SLAs), utilizando estándares para su funcionamiento.	X		X	
11	Monitoreo de infraestructura tecnológica y servicio de conectividad de 781 infocentros, gestión de despliegue de software en inventario de 8267 estaciones de trabajo que se encuentran en estos infocentros.	X		X	
12	Todo el software debe ser licenciado para un tiempo indefinido. Sin embargo se contemplará los costos de soporte técnico y actualización de versiones anualmente.	X		X	

13	Se debe prestar el servicio en la modalidad de hosting dedicado o cloud de manera que se garantice su crecimiento en componentes de infraestructura tecnológica.	X		X	
14	Se debe dimensionar el hosting dedicado del servicio en base a las necesidades resultantes del levantamiento del diseño del sistema.	X		X	
15	Proveer el procesamiento, almacenamiento, respaldo y seguridad informática para ejecutar las aplicaciones del sistema.	X		X	
16	Implementar y documentar políticas de seguridad informática para soportar los procesos de administración y monitoreo.	X		X	
17	Contemplar un plan de recuperación de desastres, el cual debe ser documentado y se realizará un simulacro mínimo 2 veces al año.	X		X	
18	Los equipos deben operar en modalidad 7X24X365, es decir 7 días a la semana, 24 horas al día y 365 días al año.	X		X	
19	El idioma del sistema debe ser en Español	X		X	
CONDICIONES ESPECIFICAS					
ÍTEM	**REQUERIMIENTO**	**CUMPLE**	**NO CUMPLE**	**CUMPLE**	**NO CUMPLE**
1	Monitorear servidores físicos y virtuales, bases de datos, aplicativos, web servers, sistemas de mail, dispositivos de red, firewalls y load balancers, que formen parte de la solución de la infraestructura a ser proporcionada.	X		X	
2	Almacenamiento de métricas monitoreadas durante al menos 6 meses y debe generar gráficos y reportes personalizables.	X		X	
3	Monitoreo de disponibilidad y el tiempo de respuesta de procesos que utilicen protocolos y servicios estándares de red como: DNS, DHCP, SMTP, HTTP, HTTPS, IMAP, POP3, FTP, entre otros.	X		X	
4	Consolas de operación con interface web.	X		X	
5	Presentación de estadísticas de los servicios de TI que se ofrecen a los usuarios Institucionales, las métricas yKPIs que definen la salud del servicio y los elementos de TI y de la red de comunicaciones que lo componen.	X		X	
6	Las métricas comunes o habituales deben estar predefinidas nativamente en la solución y deben ser fácilmente expandibles para incluir nuevas métricas a monitorear.	X		X	
7	Permite establecer los rangos de comportamiento normal, de alerta y crítico de todas las métricas monitoreadas, tanto sean métricas monitoreadas en forma nativa por la solución o sean métricas predictivas definidas a posteriori. A este comportamiento normal se lo definirá como parámetros de referencia o línea base (baseline).	X		X	
8	Los sensores o módulos de monitoreo deben registrarel comportamiento de las métricas durante los distintos momentos del día y los distintos días de la semana, con al menos una granularidad horaria.	X		X	

9	Debe generar alertas, notificaciones y eventos a través de umbrales definidos previamente y realizar notificaciones basadas en la frecuencia de repetición de los eventos registrados, en un período de tiempo o como combinación de ambos. Esta herramienta deberá ser nativamente integrada (mismo fabricante) con la Mesa de Servicios para la creación de tickets generados en forma manual o automática en función de eventos ocurridos.	X		X	
10	Los sensores o módulos de monitoreo deben tener al menos 3 estados. Ejemplo: Normal, Alerta y Crítico	X		X	
11	Generación de alertas predictivas, mediante el uso de los algoritmos estadísticos y los umbrales predefinidos, tanto superiores como inferiores, identificando tendencias de problemas en el rendimiento de la infraestructura de TI y/o de la red de telecomunicaciones monitoreada. Esto implica que a pesar de que las métricas no superan los umbrales definidos, se observa una tendencia que puede indicar un problema en próximos intervalos de tiempo, definidos en el módulo predictivo.	X		X	
12	Alertas de tendencias en el comportamiento, para lo cual se requiere el establecimiento de umbrales, los cuales mediante políticas generales o por medio de operaciones masivas, el sistema de monitoreo debe reportar que una métrica está fuera del rango normal de operación, tanto sea por encima o por debajo. Debe hacerlo en forma selectiva para las métricas monitoreadas.	X		X	
13	Ante alertas de tendencias en el comportamiento de la infraestructura y servicio monitoreado, debe poder ejecutar acciones correctivas, previamente configuradas (Ejemplo: hacer restart de proceso automáticamente).	X		X	
14	Ante alertas o eventos debe poder notificar a personas o grupos de personas a través de un mensaje de correo electrónico o un SMS opcional, manejando niveles de escalamiento.	X		X	
15	Facilidad de análisis de causa raíz, ante la caída o degradación del performance de un servicio o elemento TI, debe correlacionar las métricas y eventos existentes para determinar el posible componente de infraestructura que origina la falla.	X		X	
16	Control de acceso para los usuarios. Debe poder definir a que grupos lógicos puede acceder cada usuario y que acciones puede realizar.	X		X	
17	Soportar varios métodos de monitoreo, como : SNMP, v1,v,2,v3; JMX, WMI, SQL Query, etc.	X		X	
18	Correlación de eventos en cascada para las alarmas, para suprimir falsos positivos. Ejemplo: Si un Web server no responde al comando ping, todas las alertas de transacciones Web de ese web server, deben ser escondidas.	X		X	
19	Se podrá representar cualquiera de los parámetros monitoreados mediante gráficos desde la consola Web	X		X	
20	Debe permitir agrupaciones lógicas de los elementos monitoreados y la definición de funciones o servicios virtuales a los cuales se les pueda dar niveles de importancia o pesos que permitan cuantificar el impacto o la afectación de los servicios en cada uno de los eventos.	X		X	
CONSOLA DE OPERACIÓN					

21	Presentación a través de una interface Web	X		X	
22	Visualización del estado actual de los elementos monitoreados	X		X	
23	Visualización y administración de alertas	X		X	
24	Visualización del comportamiento histórico de las métricas mediante gráficos	X		X	
25	Consulta de métricas en tiempo real	X		X	
26	Generación y personalización de reportes	X		X	
27	Definición y modificación de umbrales	X		X	
28	Consulta y definición de SLAs	X		X	
29	Definición de alertas y reglas de notificación	X		X	
30	Manual de acciones de recuperación de la herramienta	X		X	
31	Cada usuario debe poder personalizar su consola de operación de forma independiente	X		X	
MANEJO DE ALERTAS Y EVENTOS					
32	Visualización de eventos activos y cerrados	X		X	
33	Registro de la fecha y hora de la alerta	X		X	
34	Elemento afectado y evento generado	X		X	
35	Diferenciación del estado de la alerta: activa, cerrada, trabajando, etc.	X		X	
36	Configuración de criticidad de los estados (normal, alerta, crítico)	X		X	
37	Permitir identificar alertas que estén asociadas al evento correspondiente	X		X	
38	Permitir marcar un evento de tal forma que indique que se está trabajando en él	X		X	
39	Permitir asociar comentarios al evento por parte de los operadores	X		X	
VISUALIZACIÓN DE GRÁFICOS DE MONITOREO					
40	Generación de gráficas tipo: lineal, área, X-Y, torta y sobre mapas GIS o de red.	X		X	
41	Manejo de varios indicadores diferentes en un gráfico (Ej.: % y Tiempo de Respuesta). Así como también representar por medio de iconos los colores y estados de los diferentes componentes que están siendo monitoreados.	X		X	
42	Debe poder graficar una métrica junto con sus parámetros de referencia en el mismo gráfico, tanto numéricos como de información textual.	X		X	
43	Exportar los datos de los gráficos.	X		X	
44	Permitir agregar textos descriptivos a los gráficos, para su mejor comprensión.	X		X	
45	Restricción de gráfico a un sub-periodo de tiempo definido por ventanas o intervalos de tiempo seleccionados.	X		X	
46	Visión de "Tablero de Control", con los indicadores principales de los componentes y/o servicios monitoreados los mismos que deben ser personalizables.	X		X	
47	Cada uno de los indicadores deben poder mostrar el estado actual e histórico de las métricas	X		X	
48	Los tableros de control deben actualizar los indicadores de forma automática.	X		X	

MÉTRICAS DE REFERENCIA					
49	Registro por medio de plantillas, políticas de administración y operaciones masivas el comportamiento normal, de alerta y crítico de todas las métricas monitoreadas.	X		X	
50	Los parámetros de referencia deben mostrar el comportamiento de las métricas, con al menos una granularidad horaria.	X		X	
51	Cálculo sintético o predictivos en base al comportamiento histórico.	X		X	
52	Los módulos sintéticos o predictivos deben seguir ajustándose en forma automática con el tiempo, con la evolución de los datos históricos.	X		X	
53	Configuración de la forma de calcular los módulos o sensores predictivos.	X		X	
DEFINICIÓN DE UMBRALES					
54	Definición de umbrales estáticos con valores fijos.	X		X	
55	Definición de módulos predictivos, que debe mostrar los rangos aceptables. La presentación de los datos y el monitoreo debe ser en intervalos de tiempo definidos.	X		X	
56	Al definir módulos sintéticos, debe permitir que los valores dentro de rangos de funcionamiento normal tengan un margen de tolerancia con respecto a la referencia.	X		X	
57	Debe tener al menos 3 estados de los sensores o módulos(Ej.: normal, alerta y, crítico)	X		X	
ARQUITECTURA Y ADMINISTRACIÓN					
58	Arquitectura escalable que permita el crecimiento del sistema.	X		X	
59	La base de datos debe tener un esquema abierto que permita el acceso de herramientas de generación de reportes.	X		X	
60	Permitir el monitoreo remoto, no necesariamente desde un servidor central.	X		X	
61	Incluir un sistema de firewalls.	X		X	
62	Configuración de los agentes de monitoreo debe ser centralizada.	X		X	
63	Puertos de interconexión entre el servidor y los agentes, que se utilizan para realizar control y acceso remoto, deben poder ser configurables.	X		X	
64	Comunicación entre el servidor y los agentes debe ser encriptada.	X		X	
SEGURIDAD Y ACCESO					
65	Se debe manejar restricciones de seguridad en el control de acceso en función de los roles.	X		X	
66	Debe manejar un control de acceso por usuario.	X		X	
67	Debe permitir crear grupos lógicos para el manejo de reglas.	X		X	
ACUERDOS DE NIVELES DE SERVICIO					
68	Definición y registro de SLA en base a las métricas monitoreadas de los componentes de infraestructura y conectividad.	X		X	
69	Debe poder definir SLAs en base a los contratos y convenios existentes, tomando como referencia los servicios que puedan ser monitoreados en forma automática.	X		X	
70	Se deben definir niveles porcentuales de cumplimiento.	X		X	

71	Debe realizar un registro del cumplimiento de los SLA.	X		X	
72	Debe registrar fecha y duración del incumplimiento del SLA.	X		X	

4.4. SOLUCIÓN APLICADA.

El Ministerio de Telecomunicaciones y Sociedad de la Información requiere el "DISEÑO DE UN SISTEMA DE GESTIÓN, CONTROL Y MONITOREO PARA LA RED DE INFOCENTROS A NIVEL NACIONAL" que permita cumplir con los siguientes objetivos:

- Contar de un Centro de Gestión de Servicios de las Tecnologías de Información, que incluya las funciones de Monitoreo y Mesa de Servicios, el mismo que servirá para controlar el funcionamiento adecuado de 781 Infocentros y Megainfocentros, los mismos que tienen instalados un total de 8081equipos (3920 PC, 3870 Thin Clients y 291 servidores.
- Se requiere realizar el monitoreo de la disponibilidad del ancho de banda de internet que ha sido instalado en los centros, generando reportes de cumplimiento del servicio SLAs, de manera que sirvan como respaldo para los desembolsos realizados mensualmente a los proveedores correspondientes. En forma complementaria, se requiere determinar el ancho de banda disponible y la utilización de tales canales de comunicaciones de internet.

Implementación de un Centro de Gestión de Servicios de las Tecnologías de Información, que incluya las funciones de Monitoreo y Mesa de Servicios, el mismo que servirá para controlar el funcionamiento adecuado de 781 Centros (Infocentros y Escuelas), los mismos que tienen instalados un total de 8600 computadores el primer año, se espera llegar en una siguiente fase a un total de 60.000 computadores monitoreados.

Se requiere realizar el monitoreo de la disponibilidad del ancho de banda de internet que ha sido instalado en los centros, generando reportes de cumplimiento del servicio SLAs, de

manera que sirvan como respaldo para los desembolsos realizados mensualmente a los proveedores correspondientes. En forma complementaria, se requiere determinar el ancho de banda disponible y la utilización de tales canales de comunicaciones de internet.

El sistema de sistema de gestión, control y monitoreo para la red de infocentros a nivel nacional permitirá realizar en forma automática un registro del inventario, tanto de hardware como de software existente en los centros y facilitará el control y administración de los activos existentes.

Este proyecto se contempla para una implementación en la modalidad de servicios, es decir que la responsabilidad es del oferente bajo la supervisión y en coordinación con el Ministerio de Telecomunicaciones y Sociedad de la Información, por lo tanto se deberá contemplar la infraestructura requerida en modalidad de "hosting", de manera que cuente con medidas de contingencia que permitan asegurar la continuidad del servicio y la recuperación de eventos de desastre. Además el software incluido en la solución debiendo ser instalado y configurado para garantizar la confiabilidad e interoperabilidad del sistema en su conjunto.

A continuación se describen cada uno de los requerimientos para el cumplimiento del presente proyecto:

4.4.1. CONDICIONES GENERALES

Alineación con los siguientes procesos de ITIL: (EV) Administración de Eventos, (IM) Administración de Incidentes, (KM) Administración del Conocimiento, (SACM) Administración de Servicios y Configuraciones, (SCM) Inventario del Catálogo de Servicios registrado, (SLM) Información para Control del Cumplimiento de los Niveles de Servicio.

El diseño de un sistema de gestión, control y monitoreo para la red de infocentros a nivel nacional se basa en los productos de Ártica Soluciones Tecnológicas: Pandora FMS e IntegriaIMS, con los cuales se realizará la Gestión de Inventarios de Hardware y Software, Control Remoto, Registro de Cambios y Configuraciones, Registro de Eventos, Gestión de Incidentes, Gestión de Activos y herramientas de monitoreo, tanto pasivo como proactivo de las plataformas.

La Gestión del hardware debe incluir un inventario del equipamiento informático con las capacidades de los computadores instalados en los centros, los mismos que tienen sistema operativo LINUX UBUNTU o en algunos casos inicialización dual con el Sistema Operativo Microsoft Windows, tales como: tipo y velocidad de procesador, capacidad de discos fijos, capacidad de memoria RAM. En cuanto al software se requiere el inventario del software instalado teniendo en cuenta las versiones y licencias correspondientes, las mismas que deberán ser tomadas de los registros de los computadores en forma automática, o digitadas por operadores.

El sistema deberá permitir establecer parámetros de configuración de umbrales de operatividad, correlación de eventos y definición de mapas GIS, de redes y de los servicios que se definan por parte de los operadores, los mismos que serán presentados en consolas visuales de los operadores y también en pantallas de visualización permanente.

Se incluye la configuración, descubrimiento y población de la base de datos de configuración (CMDB), que permitirá registrar el equipamiento del Core Tecnológico con sus aplicativos e infraestructura relacionada.

Implementación del hardware y software necesarios para el Centro de Control y Monitoreo (CCM) del MINTEL que incluye licencias de IntegriaIMS para 10 operadores con

funcionalidades de Administración de Proyectos, Soporte y Gestión de Tickets para realizar el “Service Desk” (Incidentes y Problemas), Administración de Inventarios para “Change” (Gestión de Cambios) y “Asset” (Gestión de Activos) y además incluye las funcionalidades de Clientes, Personas y Wiki como base de conocimientos. Este proyecto además incluye la administración de sensores y la generación de reportes SLAs desde Pandora FMS para proveer el “Service Level” (Gestión de SLAs).

Despliegue del software de monitoreo e inventario en los Infocentros y Megainfocentros, para lo cual se deberán realizar los procesos de evaluación, normalización de nomenclatura de equipos y direcciones IP de las redes de datos utilizadas y también la administración del personal de instalaciones y configuración de los agentes de monitoreo. Lo cual permita registrar además la localización geográfica de cada uno de los centros en los mapas GIS de Pandora FMS. Es importante mencionar que el proceso de normalización o estandarización de nombres y direcciones IP, es clave para una efectiva monitorización y mantenimiento del inventario.

Todo el software incluido en este diseño deberá ser licenciado por tiempo indefinido, solamente es necesario considerar que los periodos de soporte y actualización de versiones son anuales. En el análisis económico se deberá incluir los costos el valor de las licencias que además incluyen el soporte y actualizaciones por 3 años.

El presente diseño contempla la modalidad de “hosting dedicado o cloud”, acorde a las condiciones de los proveedores de este tipo de servicio a nivel nacional, los precios deberán ser incluidos en el mismo, corresponden a todos los servicios de la infraestructura requerida para el cumplimiento de los requerimientos especificados.

La contratación del hosting correspondientes deberá ser presentada y aprobada por MINTEL.

El diseño planteado incluye políticas de seguridad como enlaces dedicados, firewalls y sistemas operativos de alto nivel de seguridad que permitirán soportar los procesos de administración y monitoreo.

Los equipos servidores y los canales de comunicación propuestos para el diseño de esta solución deberán funcionar en una modalidad de 7x24x365.

4.4.2. MONITOREO PROACTIVO

El diseño presentada una solución integral, pues incluye monitoreo proactivo, control de disponibilidad, rendimiento, usabilidad de recursos y tiempo de respuesta de la infraestructura de TI, de la red de comunicaciones y de los servicios brindados. Permite el monitoreo de servidores físicos y virtuales, bases de datos, aplicativos, servidores web de internet o de intranet, sistemas de correo electrónico, dispositivos de red, firewalls y balanceadores de carga; los cuales pueden estar dentro o fuera de la infraestructura a ser proporcionada.

La base de datos de Pandora FMS, viene configurada de fábrica para almacenar las métricas monitoreadas por un periodo de 3 meses, sin embargo de lo indicado, es posible configurar un servidor de base de datos histórica que incluya la información de más largo plazo y que dependerá del espacio en disco asignado. Para este diseño se contempla la utilización de una configuración en que la información en la BDD principal contenga la información del último mes, con transferencias semanales de los datos al histórico, que podrá contener la información de al menos un año, de manera que se puedan hacer reportes y gráficas de

todo el año y además proyecciones de tendencias en las métricas con información histórica de un año.

Los módulos de red de Pandora FMS permiten realizar monitoreo de protocolos y servicios estándares, tales como: DNS, DHCP, SMTP, HTTP, HTTPS, IMAP, POP3, FTP, entre otros. Los cuales pueden ser evaluados por sí mismos de acuerdo a la existencia de los "daemon" o procesos correspondientes en el sistema operativo o mediante la actividad de los puertos de comunicaciones utilizados y también por medio de evaluación de resultados, realizando pruebas temporizadas de funcionamiento, de manera que se pueda certificar que se encuentran funcionando correctamente y que los tiempos de respuesta son adecuados.

Tanto la consola de Pandora FMS como la meta consola, son aplicativos con interface web, que puede ser utilizada desde la intranet o internet, utilizando puertos no seguros (HTTP: Puerto 80) o puertos seguros (HTTPS: Puerto 443).

Los agentes incluyen módulos previamente establecidos, los mismos que tienen definidos rangos de comportamiento normal, alerta y críticos, dependiendo de su naturaleza. Sin embargo es posible definir nuevos, los mismos que pueden ser activados en sitio, o remotamente desde la administración central. Adicionalmente, es posible definir políticas y operaciones masivas, que permiten aplicar nuevos sensores o módulos a todos los elementos monitorizados o a grupos de acuerdo a la definición adoptadas.

Las alertas, notificaciones y eventos se pueden definir previamente o en forma personalizable, lo cual facilita su administración y la aplicación correspondiente en grandes volúmenes de equipos administrados.

Pandora FMS puede generar módulos predictivos que permiten evaluar tendencias de comportamiento, los mismos que toman los datos de módulos que ya cuentan con datos

históricos y en base a los cuales se pueden observar los valores futuros en base a cálculos estadísticos, generando además alertas predictivas, que podrían servir para temas como por ejemplo “capacityplanning”.

Ante la presencia de alertas o eventos producidos, o alertas de tendencias, se puede configurar notificaciones individuales, de grupos y con escalamiento. Además se pueden generar acciones correctivas, que serán previamente configuradas en base a comandos del sistema operativo o “plugins” existentes ya en las librerías de la solución.

Este sistema, permite definir reglas lógicas entre los eventos del sistema, basados en varios campos, como “tag”, estado, criticidad, valor, grupo o agente de origen, etc. Todas estas reglas además se aplican sobre una ventana de tiempo. Este sistema permite “filtrar” falsos positivos, tormentas de eventos y poder determinar la causa raíz del problema de una forma más automatizada y clara.

Los usuarios y operadores ingresan con un “login” y “password” definidos, los cuales les permite ingresar mediante una interface web a la consola de administración y monitoreo. Las capacidades asignadas a los usuarios dependen del grupo lógico en el que se encuentren y de las autorizaciones asignadas a este grupo.

Existe una infinidad de módulos de monitoreo definidos en las librerías de Pandora, los mismos que incluyen entre otros: SNMP, v1, v2, v3, componentes Java como JMX y log4j, WMI para monitoreo de equipos Windows, consultas a diferentes tipos de bases de datos, como Oracle, MySQL, Postgress, SYBASE, MS-SQL Server, etc.

La consola web permite definir y presentar diferentes gráficos de parámetros o sensores monitoreados, entre los cuales se puede mencionar: Mapas GIS o Geográficos, Mapas de Red, Mapas de Servicios, Gráficos de módulos, Reportes Gráficos generados en línea. Es

importante mencionar que la consola de Pandora facilita la creación de nuevos gráficos desde plantillas existentes o también permite la incorporación de nuevos gráficos, cuando los existentes no cumplan con los requerimientos planteados.

La solución permite definir servicios lógicos, que conforman la estructura virtual de las funciones realizadas, estos elementos facilitan las agrupaciones lógicas de los servicios de TI y su administración, control y reacción ante las diferentes situaciones que puedan existir.

4.4.3. MONITOREO DE INFRAESTRUCTURA DE TI

El diseño incluye capacidades para el monitoreo de todos los componentes de la infraestructura de TI que forman parte de la solución y para las redes de telecomunicaciones que forman parte de este alcance.

Todas las métricas nuevas podrán ser usadas por la solución con las mismas capacidades que las métricas pre-existentes. Es decir, guarda un historial, muestra gráficos sobre las mismas, define umbrales de normalidad, alerta y críticos, los cuales pueden ser utilizados para el análisis de causa raíz, generar gráficos y reportes.

Permite el uso de modelos genéricos o establecidos, que pueden ser aplicados a nuevos agentes o elementos a monitorear. Adicionalmente se pueden aplicar en operaciones masivas o como parte de la definición y aplicación de políticas.

Utiliza umbrales configurables sobre módulos predictivos, de manera que pueden proyectas el comportamiento futuro de un módulo existente. Tanto los módulos predictivos como los módulos originales o básicos son configurables desde la consola.

Permite el monitoreo del protocolo SNMP v1, v2 y v3. Adicionalmente permite realizar el barrido SNMP, el descubrimiento de OIDs y además se puede hacer la carga de bases de

datos MIB que contengan la información de monitoreo existentes en equipos originalmente no considerados en la base de monitoreo. Permite además la recepción de trapsSNMP de manera que se pueda realizar monitoreo asincrónico de equipos que tengan esas capacidades.

4.4.4. CONSOLA DE OPERACIÓN

La consola de operación y la meta consola tienen una interface web, que puede accederse desde equipos con navegadores de internet, la misma que permite la visualización del estado actual e histórico de los agentes monitoreados. Visualización y administración de alertas.

El comportamiento histórico de las métricas se puede observar mediante gráficos configurables y mediante tablas de datos.

Las consultas de las métricas se realizan en tiempo real, es decir que pueden ser observadas y procesadas tan pronto como son recibidas de los agentes.

La consola de operación facilita la generación y personalización de reportes, los mismos que pueden ser construidos en base a “wizards” y también mediante las modificaciones manuales que facilitan su adaptación a las necesidades de los operadores.

Adicionalmente la consola permite la definición y modificación de umbrales, consulta y definición de SLAs, definición de alertas y reglas de notificación, que permiten realizar el escalamiento necesario en caso de reincidencia de los eventos por intervalos de tiempo.

La consola permite además acceder a todos los manuales de operación existentes, entre los cuales se incluyen acciones o procedimientos para solucionar problemas de la herramienta,

entre otros documentos que van desde los procedimientos de instalación y configuración hasta la operación con mecanismos avanzados.

La consola tiene opciones de configuración, que incluye “look and feel”, idioma de presentación, colores, sonidos, zonas horarias, uso de http o https, etc.

4.4.5. MANEJO DE ALERTAS Y EVENTOS

Permite la visualización de eventos activos y cerrados, la fecha y hora en la que se produjo la alerta, los elementos que intervienen en el evento, es decir el módulo que generó el evento dentro del Agente correspondiente.

Los eventos tienen una clasificación dependiendo del estado en la que se encuentran: activo (nuevo), cerrado (validado), trabajando (en proceso), etc. Las alertas pueden ser definidas en función de plantillas que pueden ser catalogadas como: normal, alerta, crítica, etc.

La gravedad de los eventos puede ser informativo, menor, mayor, crítico.

Se puede identificar la alerta que ha sido asociada al evento correspondiente.

Permite marcar a un evento para identificar que se está trabajando sobre él, además permite el ingreso de comentarios al evento por parte de los operadores, de manera que se convierte en una base de conocimientos de las acciones aplicadas y de las personas que han actuado sobre él.

4.4.6. VISUALIZACIÓN DE GRÁFICOS DE MONITOREO

Permite la generación de gráficas de diferentes tipos, dependiendo de las métricas que se desea representar, por ejemplo: lineal, área, X-Y, stack line y stackárea, pasteles, etc. Las mismas que pueden ser combinadas para mostrar diferentes medidas en un solo gráfico y

con eso lograr la comparación cuando es necesaria. Adicionalmente permite la presentación de los datos mediante "zoom" a diferentes niveles, lo cual facilita la apreciación de detalles. En otros escenarios, es necesario mostrar las gráficas sobre mapas GIS o geográficos y también sobre mapas en los cuales se presentan topologías de red. Estos gráficos pueden ser combinados con otros, en los dashboards para dar una perspectiva completa y de un solo vistazo de la situación de los elementos monitorizados, permitiendo además incluir otros elementos que den la perspectiva global del funcionamiento, todo esto facilitando además el acceso a los elementos de detalle correspondientes, mediante una selección simple.

Dentro de cada gráfico se pueden presentar diferentes indicadores, los cuales son seleccionados por el operador al momento de diseñarlos, facilitando de este modo la inclusión de porcentajes, tiempos de respuesta, etc. Adicionalmente, en las gráficas se pueden incluir diferentes tipos de iconos con colores y estados que reflejen su situación actual. Además es posible incluir información de texto o numéricos, tales como títulos, comentarios y datos generales que pueden ser de ayuda e identificación.

Los datos de los gráficos pueden ser exportados a diferentes formatos como HTML, XML, CSV o PDF.

Como se ha mencionado anteriormente, es posible añadir textos descriptivos a los gráficos, lo cual permite su mejor comprensión.

Los gráficos pueden ser presentados seleccionando sub-periodos de tiempo los cuales se definen en función de ventanas o intervalos de tiempo seleccionados en base a la fecha de inicio y al intervalo de tiempo que se desea presentar.

Los “Tableros de Control” de Pandora o “dashboards” son personalizables y permiten la presentación de todo tipo de indicadores, tanto de alto nivel como de detalle. Adicionalmente se pueden presentar en modalidad de “diapositivas”, los mismos que pueden mostrar un conjunto de indicadores en una pantalla que se presenta en un intervalo corto de tiempo, por ejemplo 5 o 10 segundos y luego pasa a la siguiente diapositiva, que puede contener otros indicadores. El operador decide cuantas diapositivas desea presentar en un dashboard de control.

Los indicadores muestran tanto los estados actuales como los históricos de las métricas, tanto en forma gráfica, como también en forma de un cuadro de datos.

Los dashboard de control actualizan los indicadores en forma automática, en base a un tiempo de refresco que es configurable.

4.4.7. MÉTRICAS DE REFERENCIA

Los módulos o sensores de Pandora pueden ser creados en forma individual con sus métricas default. Pero además es posible crear módulos en base a plantillas, políticas de administración y operaciones masivas, asignándoles umbrales de funcionamiento de acuerdo a las condiciones requeridas de monitoreo. Adicionalmente es posible crear módulos sintéticos que realicen cálculos o registren tendencias o estadísticas de comportamiento de otros módulos previamente configurados.

Las métricas registradas en los módulos o sensores se registran con una frecuencia de barrido, la cual viene configurada de fábrica en 5 minutos. Este valor puede ser cambiado en la configuración. Por lo cual se puede considerar, que el registro de las métricas tiene una granularidad de unos pocos minutos. En caso de ser necesario se puede configurar también para que tenga un barrido de horas.

Pandora en su versión Enterprise, incluye un servidor predictivo, que permite la creación de módulos sintéticos o predictivos, los mismos que son configurados para registrar información generada mediante cálculos o estadísticas tomadas de otros módulos, los mismos que pueden ser, módulos simples o módulos de servicios de alto nivel. De esta forma pueden irse ajustando en función del tiempo.

Los módulos o sensores predictivos son configurados por los operadores y su funcionamiento depende de las fórmulas aplicadas, las mismas que pueden ser modificadas para irse adaptando a las necesidades de cada instalación.

4.4.8. DEFINICIÓN DE UMBRALES

Los módulos o sensores de la solución permiten la definición de umbrales estáticos con valores fijos, los mismos que pueden ser registrados durante la creación del módulo o mediante la configuración en el agente remoto.

La definición de los módulos predictivos, permite registrar los valores aceptables. La presentación de los datos y el monitoreo se realizan en intervalos de tiempo denominados barridos, que por configuración de fábrica se realizan cada 5 minutos

Los sensores y módulos tienen al menos 3 estados: Normal, alerta y crítico.

4.4.9. ARQUITECTURA Y ADMINISTRACIÓN

La arquitectura del diseño es muy escalable, permitiendo un crecimiento casi lineal en función del incremento de servidores. Se considera adecuado asignar unos 2000 Agentes por servidor de monitoreo, pudiendo en algunos casos llegar hasta 3000 Agentes sin mayores afectaciones de rendimiento.

La base de datos donde se almacena la información de Pandora es MySQL, la misma que tiene un esquema abierto, permitiendo el uso de cualquier mecanismo de acceso para la obtención de los datos almacenados.

La monitorización se puede realizar tanto desde los servidores de Pandora, como de la metaconsola en forma local o remota a través de una interface web, a la misma que se puede ingresar por medio de un login y password provisto a los operadores.

En la configuración de la arquitectura de este proyecto se incluyen al menos dos firewalls que servirán como control de acceso a los servidores que realizan el monitoreo.

La configuración de los agentes de monitoreo, puede ser realizada de manera local en cada agente, como también centralizada en la metaconsola de administración de Pandora.

Para realizar procesos de administración y control remoto, se puede utilizar opciones incorporadas en la interfaz de Pandora como son: Escritorio remoto mediante VNC o Team Viewer, así como también mediante SSH o TELNET. Para conectarse mediante estas herramientas se puede configurar los puertos correspondientes.

La comunicación entre el servidor y los agentes puede ser en modo encriptado utilizando HTTPS (SSL) y también utilizando el protocolo Tentacle mediante SSL.

4.4.10. SEGURIDAD Y ACCESO

Permite manejar restricciones de seguridad en el control de acceso en función de roles o grupos de usuarios, así como también en base a la definición de grupos de recursos que son monitorizados en el sistema.

Permite el control de acceso por usuario, el mismo que debe suministrar su login y password para acceder a la consola de monitoreo. Los usuarios y sus claves pueden estar registrados en la Base de Datos de Pandora o en un servidor de Dominio LDAP.

Pandora permite la creación de grupos lógicos de recursos, sobre los cuales se realizan los procesos de administración y control, así como también la asignación a los usuarios.

4.4.11. ACUERDOS DE NIVELES DE SERVICIO

Pandora permite definir reportes de SLAs, los mismos que presenten las métricas monitoreadas y su cumplimiento, de manera que puedan ser incluidos en informes gerenciales, generados automáticamente con varios elementos de monitorización,

Los SLAs podrán ser definidos en base a la información contenida en contratos y convenios existentes, tomando como referencia los datos almacenados en los módulos monitorizados.

El cumplimiento es registrado en función de niveles porcentuales.

Los informes presentan el cumplimiento o falta de cumplimiento de los SLAs definidos

Se puede observar además tablas de los valores obtenidos, de manera que se identifique las fechas y duraciones de los incumplimientos producidos.

4.4.12. MAPA DE SERVICIO

Pandora permite la presentación de mapas geográficos que incluyen los centros monitorizados a partir de la información cargada en la CMDB. Adicionalmente permite registrar las posiciones geográficas tanto desde los agentes, como también desde la consola de administración y monitoreo.

Facilita la creación de modelos de dependencia de servicios que presente a nivel lógico las relaciones entre los servicios y sus componentes. Es decir que facilita la creación de mapas de servicios.

Los mapas de servicio pueden ser observados por los operadores, considerando los niveles y las autorizaciones correspondientes.

Los mapas de servicios reflejan el estado de los servicios y cada uno de sus componentes empleando códigos de colores. El refrescamiento de los mapas es definido por los operadores del sistema.

Los elementos del mapa de servicio muestran su estado actual, si se selecciona el elemento, permite observar la información detallada del mismo.

Utiliza mapas gráficos que permiten relacionar los servicios de TI, localizaciones físicas y presentar los gráficos de los módulos con información de los niveles de servicio aplicables.

Los gráficos de servicios permiten mostrar los diferentes elementos, incluyendo sus estados y permiten acceder a los elementos de niveles inferiores que presenten los componentes a mayor detalle. Los gráficos se refrescan a intervalos de tiempos definidos por el usuario. La interfaz gráfica facilita el descubrimiento del recurso que está siendo monitoreado de TI o de la red de comunicaciones que causa la interrupción del servicio.

Los usuarios operadores están en capacidad de ingresar vía una interfaz web, la misma que tiene un control de autenticación con usuario y password y seguridades de acceso en base a roles o perfiles.

Provee un entorno gráfico web que facilita el desarrollo y administración de todas las operaciones, incluso los modelos o configuraciones de servicios.

Se provee integración nativa entre los componentes de la solución, lo cual permite realizar operaciones de gestión de incidentes y eventos.

Pandora incluye la definición de mapas de red, los cuales representan los recursos de la red de telecomunicaciones que brinda el servicio, como son: aplicativos, servidores, bases de datos y dispositivos de red.

Los componentes a ser presentados en los mapas corresponden a recursos lógicos o físicos, tales como grupos de usuarios, regiones geográficas y procesos de negocio.

Cuando algún componente es afectado por una falla en alguno de sus módulos, se lo observa con un distintivo con colores que dependen del estado en el que se encuentre y además sus módulos o elementos monitoreados, presentan el color distintivo que representa la situación en la que se encuentran: normal, alerta o crítico. Adicionalmente, es posible asignar distintos tipos de iconos que permitan una representación visual de la situación en la que se encuentran los agentes y módulos monitoreados.

Los componentes de las gráficas pueden ser relacionados entre sí, por medio de líneas o por medio de colores y agrupaciones, que permitan identificar la inter-dependencia entre los mismos.

4.4.13. MESA DE AYUDA (SERVICEDESK)

La solución permite la asignación del número de ticket o de caso para las solicitudes de usuarios realizadas vía telefónica, correo electrónico o web.

Se registra la identificación del usuario la primera vez que llama al centro de monitoreo, tal información queda registrada en el sistema, de manera que pueda ser utilizada en

operaciones posteriores. La información a ser registrada podrá ser personalizada como parte del proyecto.

Se desarrollará un módulo de encuestas personalizadas para ser enviadas al usuario final, donde se evalúe y reporte la calidad del servicio recibido.

El sistema permite categorizar las solicitudes como incidentes o requerimientos, de acuerdo al requerimiento del cliente.

Además incluye además un histórico de los eventos reportados por los usuarios, del cual se pueden extraer consultas como: eventos reportados con mayor frecuencia por parte de los usuarios.

La solución incluye información de los niveles de servicios aplicables, de tal manera que permitan generar las notificaciones de los eventos de acuerdo a su criticidad, ya sean estos requerimientos o incidentes.

Se puede realizar la asignación automática de los eventos al operador en base a grupos que identifican el nivel de soporte y dentro de ellos a la carga de trabajo de cada uno de los operadores.

Se puede realizar comunicados de alerta por correo electrónico a grupos de usuarios o a usuarios individuales.

La arquitectura de este proyecto ha sido definida considerando criterios de alta disponibilidad de los servicios provistos.

4.4.14. GESTIÓN DE INCIDENTES

Para cada evento se asigna un número de ticket o identificador único que permite realizar el seguimiento del requerimiento, desde el momento en que es reportado, hasta cuando se registre su solución y cierre correspondiente.

Se registra la información básica del incidente, incluyendo: nombres del usuario, detalle del incidente, fecha y hora, categorización del evento y los detalles de la solución.

Las nuevas incidencias son procesadas como eventos, los mismos que pueden ser procesados para enviar notificaciones a los usuarios operadores y administradores del sistema cuando se registren nuevas incidencias.

Los incidentes se pueden clasificar por el nivel de criticidad. En IntegriaIMS se utilizan al menos 5 niveles de criticidad, los mismos que son: Mantenimiento, Informativo, Bajo, Medio, Serio y Muy Serio.

Los incidentes se registran en la Base de Datos Central MySQL. Se puede hacer búsquedas de los eventos tanto por cualquiera de los campos registrados, como también por medio de strings de búsqueda de contexto.

Las acciones aplicadas a los incidentes se registran en el Wiki o Base de conocimientos, que permite hacer búsquedas, que permiten hacer un seguimiento de las diferentes acciones requeridas para llegar a la solución del caso. Los campos son incrementales de manera que se pueden ir agregando entradas o unidades de trabajo a medida que se trabaja sobre el incidente. Se registra el usuario, la fecha y hora de trabajo y no pueden ser modificados o eliminados por medio de entradas posteriores.

La interfaz web permite a los usuarios finales, reportar, modificar y cerrar incidentes.

Los operadores que ingresan al sistema, son registrados en un archivo log o en la base de datos.

Se puede configurar los tipos de tickets, por ejemplo: de acuerdo a la afectación, como indisponibilidad parcial, intermitencia de servicio, indisponibilidad total, etc.

Los estados de los incidentes pueden ser: Nuevo, sin confirmar, asignado, re-abierto, pendiente de cerrar, pendiente por una tercera persona y cerrado.

Permite ingresar descripciones en las que se registra las diferentes acciones realizadas como también la solución definitiva o temporal.

Permite signar las incidencias a grupos de operadores, quienes podrán tomarlos para ir resolviendo cada caso. De esta manera pueden realizar el seguimiento correspondiente los registros de cierre y las diferentes comunicaciones al usuario final.

La herramienta permite la generación de diferentes tipos de reportes, los mismos que pueden ser personalizados de acuerdo a la necesidad de los usuarios. Incluso se puede parametrizar los reportes en base a diferentes criterios y los resultados pueden ser exportables a diferentes formatos, como HTML, XML, CSV o PDF. Los archivos HTML, XML y CSV pueden ser cargados en Excel.

Como se ha indicado anteriormente, la herramienta permite asignar actividades/tareas a los operadores y hacer seguimiento de las mismas: persona asignada, estado, fechas de inicio y final.

Se puede hacer búsquedas por eventos que tengan información en común, mediante la utilización de cadenas de búsqueda.

4.4.15. GESTIÓN DE NIVELES DE SERVICIO

Permite administrar y reportar los acuerdos de niveles de servicio, mediante reportes y gráficas de los módulos sobre los cuales se hayan aplicado tales controles.

Pandora en su versión Enterprise incluye herramientas para el monitoreo y gestión de eventos, permitiendo realizar acciones de resolución de fallas de la infraestructura monitoreada basada en umbrales establecidos.

Incluye el registro y el control de los SLAs y OLAs de los módulos y sensores

Incluye la funcionalidad de control de los acuerdos de servicio y se puede generar notificaciones cuando se produzcan fallas, que permitan informar en forma automática los eventos que pueden ocasionar la superación de umbrales especificados antes del incumplimiento del acuerdo.

Permite la presentación de informes de acuerdo a los requerimientos de los SLAs, que incluyan el porcentaje de cumplimiento y el periodo aplicable.

Se puede definir en forma individual y por grupos los distintos destinos a los cuales se pueden enviar las notificaciones de los eventos que se presenten.

Tiene facilidades para consultar casos y eventos abiertos, así como también las actividades relacionadas, que permitan dar apoyo al personal de los grupos de soporte.

4.4.16. REPORTES

La personalización de este proyecto incluirá la generación de reportes estadísticos: Soportes Pendientes, Cantidad de soportes atendidos por cada agente, tipo de evento, frecuencia de un evento, eventos cerrados.

Los reportes serán fácilmente configurables y parametrizables, incluyendo además facilidades para generar los datos en archivos con formatos HTML, XML, CSV y PDF. Los archivos con formato HTML, XML y CSV pueden ser cargados en Excel.

Pandora incluye herramientas para la generación de tableros de control, con información de Indicadores Clave de Gestión (KPIs), mostrando uno o varios paneles de control con opciones gráficas que resuman la información más relevante, incluyendo facilidades de profundización de la información y navegación hacia la información de detalle.

4.4.17. GESTIÓN DE ACTIVOS

Pandora facilita la obtención del inventario de hardware y software de la infraestructura administrada por medio de su Servidor de Discovery y también por medio de los plugins de recopilación de Inventario de cada uno de los agentes.

Los plugins permiten obtener el inventario detallado de hardware en cada estación de trabajo.

Los plugins permiten obtener el inventario de software instalado, incluyendo información de sistema operativo, versión del software, etc. Adicionalmente, se pueden incluir campos personalizables que registren información relativa a las licencias del software, las cuales deberán ser registradas por los operadores.

Como se ha mencionado anteriormente, Pandora tiene una herramienta que facilita la generación de reportes de diferentes tipos por parte de los operadores.

Se pueden incluir campos adicionales que registren datos financieros del inventario registrado.

La información del inventario de hardware y software es actualizada en forma automática, cada vez que se produce un barrido y es reportada desde los agentes correspondientes.

La información para gestión del ciclo de vida de los activos, podrá ser registrada en campos adicionales, incluyendo estado (activo, inactivo, dañado, obsoleto, dado de baja), tiempo de vida, etc., los cuales dependerán de la información que se desee registrar.

La información de mantenimiento de activos se puede registrar en campos adicionales.

En el inventario se registra todo el software instalado en los equipos y que pueda ser detectado por los plugins de los agentes.

4.4.18. MEDICIÓN DE TRÁFICO

Pandora incluye una gran cantidad de mecanismos para permitir la gestión y medición del tráfico de la red de telecomunicaciones asociada al servicio de conectividad, entre los cuales se pueden mencionar los siguientes: Host Alive, Ping, Latencia, Número de octetos en las interfaces de red de entrada y salida a ser consultados mediante SNMP, plugins invasivos de medición de tráfico conectados a servidores que permiten la obtención de esa información, entre otros.

Los agentes instalados en los diferentes computadores, permitirán realizar el monitoreo de los servicios de conectividad que lo permitan, los cuales estarán distribuidos en las diversas zonas geográficas. Con tales agentes se podrá registrar el tiempo de actividad de los enlaces y presentar gráficas de estados activos e inactivos (uptime/downtime).

Para el monitoreo del ancho de banda se puede utilizar mecanismos no invasivos, como son trapsSNMP para consultas a los dispositivos; y, también se pueden ejecutar procesos invasivos como por ejemplo un plugin de speed test, que inunda el canal con tráfico hasta

obtener el máximo posible. Hay que considerar que los mecanismos invasivos no se deben ejecutar con mucha frecuencia, lo cual podría evitar que otros servicios utilicen en forma óptima el canal de datos.

Se podrán establecer mecanismos de alarma cuando se sobrepasen los umbrales definidos. Y generar alertas de los estados de las métricas monitoreadas.

Utilizando el mecanismo de Netflow en equipos Cisco o mediante los agentes “fprobe” en equipos Linux, se puede clasificar el origen y destino del tráfico de red, tanto de entrada como de salida.

Se podrán generar informes y reportes gráficos de los módulos que sensan los servicios de conectividad, los mismos que podrán ser actualizados con la frecuencia que el usuario requiera.

Como se ha mencionado anteriormente, maneja el control de autenticación y seguridad de acceso.

Incluye además el monitoreo de los servicios de comunicaciones que permiten el acceso a la solución integral de monitoreo.

4.4.19. CONTROL REMOTO

Pandora permite tomar el control remoto de las estaciones de trabajo desde la consola web de administración y monitoreo utilizando los protocolos VNC, Team Viewer, SSH y Telnet. Los cuales permiten al operador realizar operaciones como logon, logoff, reinicio del equipo, etc., a través de la sesión remota.

Las opciones de control remoto están sujetas a los niveles de acceso y a los grupos configurados de los equipos monitoreados.

La interfaz de la consola y metaconsola de Pandora es Web, que incluye además un control de autenticación y seguridad de acceso.

4.4.20. PROYECCIÓN DE VALOR ECONÓMICO

El resumen de los equipos requeridos para cumplir con las condiciones establecidas en el punto 4.1 de este documentó se definen en la siguiente tabla así como su valor económico:

ÍTEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
1	Servicio de Hostingde los Equipos	36 meses	12500	450000
2	Hardware CCM, Incluye 10 Computadores, 2 TV 50plg, equipos de comunicaciones telefónicas y red de datos	1	125000	125000
3	Licencias Pandora FMS (10000 Agentes) 3 Años de soporte	1 (10000 agentes)	215000	215000
4	Licencias Integria (10 Operadores) 3 años de soporte	10 (operadores)	11000	11000
5	Licencias MySQL Server Enterprise con soporte 3 años	3 (servidores)	28000	84000
6	Licencias Linux Enterprise, con soporte por 3 años	8 (servidores)	5000	40000
7	Capacitación ITIL	10 vouchers	4200	42000
8	Capacitación Pandora (PAT y PAE)	10 alumnos	1950	19500
9	Personalización 3 meses (4 recursos), Sistema de Encuestas e Integración de dashboards de control y estadísticas. Incluye personal de Articaon-site (Transporte, hospedaje y viáticos por un mes)	3 meses	40000 (mensual)	120000
10	Instaladores de los Agentes en los Centros (20 personas * 6 meses)	120 personas mes	850	102000
11	Gerente del Proyecto (7 meses)	1920 hora/Ing.	5000	35000
12	Ingenieros de configuración, 4 Ingenieros * 3 meses * $26/hora	7 meses	26	49920
13	Soporte Técnico 7x24x365	1920 hora/Ing.	3520	126720
14	Transporte, Movilización, Viáticos y Seguros del Personal de instalación	36 meses	204	164220
15	Gastos Administrativos	781 centros	50400	50400
16	**VALOR TOTAL SIN INCLUIR IMPUESTOS DE LEY**			1634760
17	**SON UN MILLÓN SEISCIENTOS TREINTA Y CUATRO MIL SETECIENTOS SESENTA DÓLARES CON CERO CENTAVOS**			

CAPÍTULO V:

CONCLUSIONES Y RECOMENDACIONES.

Este documento de tesis es el resultado del proceso de investigación y desarrollo, en el *"Diseño de un Sistema de Gestión, Control Y Monitoreo para la Red de Infocentros a Nivel Nacional"* a partir de la problemática identificada, se estableció una solución base a los requerimientos establecidos.

a) El diseño es una alternativa viable para los requerimientos generados en la Red Infocentros a nivel nacional, la ventaja de implementar este sistema es gestionar, controlar y monitorear la infraestructura tecnológica así como garantizar el buen desempeño de los mismos, a través de la aplicación de políticas, reglas y tareas.
b) Si además se permite a las autoridades del Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, obtener información real sobre el impacto producido por los Infocentros en las comunidades beneficiarias.

Para finalizar este trabajo de tesis, en este capítulo desarrolle las conclusiones y recomendaciones derivadas del análisis realizado en base a los requerimientos técnicos establecidos por la entidad requirente, con la finalidad de dar a conocer los beneficios que generaría la implementación de este sistema.

5.1 CONCLUSIONES:

Se obtiene primeramente como conclusión que, en la mayoría de casos las comunidades rurales y urbano marginales beneficiarias de los Infocentros poseen un bajo o nulo nivel de acceso a las TICs, dando como resultado un gran impacto de los mismos, creando una debilidad al no poseer un plan de aprovechamiento de los recursos tecnológicos existentes

y no poder optimizar los recursos instalados, ni determinar las necesidades actuales y futuras o medir y optimizar las capacidades requeridas por parte de los beneficiarios directos. Cabe destacar que uno de los puntos importantes de este diseño es el aseguramiento de la calidad a nivel nacional mediante el manejo de incidentes y promover las soluciones en el tiempo y lugar adecuado para hacer más eficiente la Gestión de TICs.

Por lo que se ha establecido la necesidad la implementación de un centro de monitoreo, administración y gestión de todos los servicios e infraestructura tecnológica basados en mejores prácticas mundiales ITIL, a nivel nacional de todas las instituciones beneficiaras, de igual manera con los proveedores del servicio; es decir contar con una herramienta para tomar decisiones acertadas y para garantizar el uso eficiente de los recursos entregados por el MINTEL, que permita obtener información actualizada y detallada sobre su infraestructura y servicios tecnológicos, sobre el uso que se le está dando a sus recursos, todo esto integrado en una sola consola de Gestión.

Adicionalmente cabe señalar que el sistema diseñado generará procesos estructurados de hardware y software adecuado que integren la gestión, administración, control y monitoreo de toda la infraestructura tecnológica entregada, así como los servicios de conectividad y demás componentes considerados dentro proyecto Infocentros, a nivel nacional, la implementación de este diseño es el primer paso para la formulación de una arquitectura de gestión de servicios, que permita generar procesos que ayuden a valorar adecuadamente los programas y su impacto en los beneficiarios y su entorno.

El modelo de gestión generado por el Sistema de Gestión, Control Y Monitoreo para la Red de Infocentros a Nivel Nacional, identificará y valorará los insumos y procesos, a fin de evaluar los resultados de los productos y servicios generados en un determinado tiempo,

de tal manera que permita medir el impacto de los programas y proyectos en el entorno económico y social, así como establecer un plan de auto sustentabilidad, ya que la base jurídica del proyecto Red Infocentros y la inversión anual del estado ecuatoriano para la sostenibilidad de los mismos, es considerable (aproximadamente USD 13.000.000,00 por año);y, que el sistema se convierta en una herramienta, para lograr que los infocentros cumplan su función, y generar instrumentos que permitan la auto sostenibilidad.

5.2. RECOMENDACIONES

Como resultado del proceso de investigación y desarrollo de este documento se establece las siguientes recomendaciones:

- Realizar las acciones pertinentes que permitan viabilizar la implementación del *"Diseño de un Sistema de Gestión, Control y Monitoreo para la Red de Infocentros a Nivel Nacional".*
- Definir las políticas y procesos mediante un conjunto de estándares que permitan administrar de manera efectiva cada uno de los procesos que son parte del proyecto, convirtiéndose en una estrategia fundamental para que el MINTEL provea valor a su servicio a través de su infraestructura.
- Socializar los beneficios que generarían la implementación del Sistema de Gestión, Control y Monitoreo para la Red de Infocentros a Nivel Nacional dado que se contará con estadísticas confiable y actualizadas sobre el impacto socio económico de la implementación de los Infocentros a Nivel Nacional.
- Analizar los contenidos y capacitaciones que se impartirán en los Infocentros ya que la herramienta diseñada de llegar a ser implementada se convertirá en un arma fundamental para conocer las necesidades específicas de cada zona del territorio

nacional, convirtiendo a los Infocentros en verdaderos centros dinamizadores de la economía social.

BIBLIOGRAFÍA.

[1] Fuente: Registro Oficial del Ecuador. Órgano del Gobierno del Ecuador, Obtenida el 22 de noviembre de 2014, de https://www.registroficial.gob.ec/

[2] Fuente: Registro Oficial del Ecuador. Órgano del Gobierno del Ecuador, Obtenida el 05 de enero de 2015, de https://www.registroficial.gob.ec/

[3] Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL. Órgano del Gobierno del Ecuador, Obtenida el 15 de enero de 2015, de http://www.telecomunicaciones.gob.ec/

[4] Fuente: Ártica Soluciones Tecnológicas. Desarrollamos software tradicional y aplicaciones móviles multiplataforma. Obtenida el 26 de enero de 2015, de http://artica.es/Home/Home/es

[5] Fuente: Kypus Nova Devices. Kypus Multifunction Security Appliance, Solución integrada de seguridad de red y comunicaciones. Obtenida el 27 de enero de 2015, de http://www.kypus.com/

[6] Fuente: Vital Innova. Vital Innova Consultores Tecnológicos, Gestión de Telecentros con Software Libre TESEO. Obtenida el 28 de enero de 2015, de http://www.vitalinnova.com/blog/gestion-de-telecentros-con-software-libre/

[7] Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL. Órgano del Gobierno del Ecuador, Proyecto Ampliación de la Red Infocentros, Obtenida el 23 de noviembre de 2014, de http://www.telecomunicaciones.gob.ec/